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

Hungary

Dr. Géza Tényi LL.M.

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?

The provisions of the Directive have already been transposed into Hungarian law with an amendment of Act C of 2003 on electronic communications (ECA). There is a pending case Nr. 568/B/2008 before the Constitutional Court of Hungary in connection with this transposition.

- ***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)?**

   Transposition has been accomplished in general, although there are no national authorities responsible for providing yearly based statistics to the Commission regarding Article 10.

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?**

   There is no public information on any drafts regarding Article 10 and statistics. Several service providers asked for a review by the Hungarian Data Protection Act (DPA), therefore an amendment is expected in 2011.

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.nhh.hu/dokumentum.php?cid=10617

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

   An amendment of the ECA has been adopted on 27th December 2007 (CLXXIV of 2007), the date of entering into force was on 15th March 2008, so there was a transition period of almost 2,5 months.

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

General rules were transposed by an amendment of ECA, the technical oriented questions were tackled by an amendment of a government's decree (180 of 2004 on the rules of cooperation between the organisations performing electronic communications tasks and the organisations authorised to collect confidential information and obtain confidential data).

The amendment of the ECA deals with the following topics:

- general provisions about how service providers have to cooporate with the National Security Agency (NSA) (ECA 92. §)
- what kind of user information should be registered in Service contract (ECA 129. §)
- how should location data processed (ECA 156.§)
- procession of users data by service provider after service (ECA 157. §)
- general rules of data retention (ECA 159/A. §)
- The amendment of the government's decree deals with the following topics:
- harmonising of legal terms with ECA
- harmonising of procedural rules with ECA

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 choosen form of transformation is correct.

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?

There are two definitions defined in the amendment of ECA and in the Directive as well:

a) the definition of location data (Article 188. point 49) it is partly the same as the Directive's definition of such data)

b) unsuccessful call attempt (Article 188. point 99/A) fully cover the definition given in the Directive

And yes, there are several other terms in connection with data retention, for examle Covert investigation, covert information gathering (Article 188. point 105)

The following definitions can be found in ECA: Identifier (Article 188. point 2); Private subscriber (Article 188. point 10); 'Subscriber (Article 188. point 22); User (Article 188. point 26); Consumer (Article 188. point 28); Mobile radio telephone service (Article 188. point 72); 'Publicly available telephone service (telephone service)' (Article 188. point 86)

Yes, there are several other terms mentioned in the given Directives – due to the fact that Hungary has already transposed the above mentioned directives into the national law. (All of the above mentioned acts and decrees and all the relavant acts will be annexed to this questioner.)

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?

According to the Article 159/A of ECA the following data have to be retained by providers:

a) the data specified in Paragraphs *b)-d)* of Subsection (6) of Section 129 related to fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these; (these are: b) the subscriber's name and address, place of abode, or registered office; c) if the subscriber is a natural person, the subscriber's birth name, and place and date of birth; d) if the subscriber is not a natural person, the subscriber's company number or other registration number, and the subscriber's current account number)

b) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, the telephone number allocated to the terminal equipment of the user or subscriber or to the subscriber access point, or the user ID or any technical identifier fixed in the subscriber contract or otherwise assigned to the subscriber or user by the provider of electronic communications services;

c) in connection with fixed network telephony services, fixed internet access services, or the combination of these, the address where the terminal equipment of the user or subscriber or the subscriber access point is installed, and the type of equipment;

d) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, the telephone numbers of the users and subscribers participating in the communication, their technical means of identification, user IDs, type of electronic communication services involved, and the data necessary to identify the date, time and duration of a communication;

e) in connection with fixed network telephony and mobile telephony services, or the combination of these, in cases involving call forwarding or call transfer, the subscriber or user number or numbers to which the call is routed;

f) in connection with mobile telephony services, concerning the equipment used at the time of communication, the International Mobile Equipment Identity (IMEI) of the calling and the called party, and the International Mobile Subscriber Identity (IMSI) of the calling and the called party;

g) in connection with mobile telephony services, the location label (cell ID) and network identifier at the start of the communication, and the data identifying the geographic location of cells by reference to their location labels (cell ID) during the period when Service was provided;

h) in connection with internet mail services and internet telephony services, or the combination of these, the data referred to in Paragraph *d)* of the intended recipient(s) of the communication;

i) in connection with internet access, internet mail services, internet telephony services, or the combination of these, type of the electronic communication service, the date and time of the log-in and log-off by the subscriber or, together with the IP address allocated to the communication, and the user ID of the subscriber or registered user, including the calling number;

j) in connection with internet access, internet mail services and internet telephony services, or the combination of these, the data necessary to trace any changes made in the unique identifiers of subscribers and users by the provider of electronic communications services (IP address, port number);

k) in the case of pre-paid anonymous mobile telephony services, the date and time of the initial activation of Service and the location label (cell ID) from which Service was activated.

The obligations in the ECA are similar to the Directive. The only difference is, according to the Hungarian regulation, more detailed information have to be retained about the users. (These are: the subscriber’s birth name, and place and date of birth; and if the subscriber is not a natural person, the subscriber's company number or other registration number, and the subscriber's current account number.)

Data on unsuccessfull calls have to be retained due to ECA 159/A. § para 2.

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.**

Yes, there are several other possibilities to retain communications data.

Order to reserve computer data

Act on criminal procedure Article 158/A. offers a possibility in order to investigate and prove a criminal offence for compulsion to reserve data, which means temporary restriction of the right of disposal of a person possessing, processing or managing data recorded by a computer system over specific computer data. The court, the prosecutor or the investigating authority shall order the reservation of computer data constituting a means of evidence or required to trace any means of evidence or the establishment of the identity or location of a suspect. From the time of being notified of the order, the obliged party, i.e. telecom provider shall reserve the data recorded by the computer system designated in the order, and ensure its safe storage, if necessary, separately from other data files. The obligation to reserve data shall be in effect until the seizure of the data, but no longer than for three months. The obligation to reserve the data shall terminate if the criminal proceeding has been concluded. The obliged party shall be advised of the conclusion of the criminal proceeding.

There has been no such official statistics published by courts, public prosecutor or any other authority on usage of these instruments, neither their success rate. As we mentioned below, lack of statistics is one of the main problems with transposition of the Directive.

Uncercover data gathering with judicial permission

On the other hand the Criminal Procedure Act Art. 200-206 allow surveillance with judicial permit, where several details are regulated by governmental decree 180/2004. In order to establish the identity, locate or arrest the offender or to find means of evidence, from the time the investigation is ordered until the documents thereof are presented, subject to a judicial permit, the prosecutor and the investigating authority may, without informing the person concerned learn and record with a technical device the contents of letters, other pieces of mail as well as communications made by way of a telephone line or other means of communication, learn and use data transmitted and stored by way of a computer system. Undercover data gathering may be applied if the proceedings are conducted upon the suspicion of a criminal offence, or an attempt of or preparations for a criminal offence which has been committed intentionally and punishable by five years' or more imprisonment, is related to trans-boundary crime, has been committed to the injury of a minor, has been committed repeatedly or in an organised manner (including criminal offences committed for profit, in a criminal organisation and conspiracy), is related to narcotics or substances qualifying as such, is related to counterfeiting of money or securities, has been committed with a weapon.

Subject of undercover data gathering may primarily be the suspect, or the person who may be suspected of having committed the criminal offence based on the available data of the investigation. Other persons may be subjected to covert data gathering, if data indicate that they have culpable communications with the person specified before or there is reasonable ground to suspect the same. The fact that an outsider is unavoidably affected shall not be an obstacle to covert data gathering. Undercover data gathering may only be conducted if obtaining evidence by other means reasonably appear to be unlikely to succeed if tried or would involve unreasonable difficulties, and there is probable cause to believe that evidence can be obtained by covert data gathering.

Last but not least anti-terrorism legislation shall be mentioned. According to Act CXXXVI of 2007 on the Prevention and Combating of Money Laundering and Terrorist Financing shall record the information regarding business relationships, the type, the subject matter and the term of the contract, regarding transaction orders, the subject matter and the value of the transaction. and Service provider may record the particulars of the transfer (place, time, mode)

According this act every person or organisation which provides one of the following services, are obligated to apply costumer due diligence measures, which means recording costumer data. The affected services are the follows:

a) provision of financial services or in activities auxiliary to financial services;

b) provision of investment services, in activities auxiliary to investment services or in providing investment fund management services;

c) provision of insurance services, insurance agency or occupational retirement provision;

d) provision of commodity exchange services;

e) service of accepting and delivering international postal money orders;

f) provision of real estate agency or brokering and any related services;

g) provision of auditing services;

h) provision of accountancy (bookkeeping), tax consulting services whether or not certified, or tax advisory activities under agency or service contract;

i) operation of a casino, electronic casino or card room;

j) trading in precious metals or articles made of precious metals;

k) trading in goods, involving a cash payment in the amount of three million six hundred thousand forints or more;

l) provision of voluntary mutual insurance fund services;

m) provision of legal counsel or notary services.

Due to Article 14 of the Regulation 1781/2006 service providers shall respond fully and without delay, in accordance with the Hungarian procedural requirements to enquiries from the authorities responsible for combating money laundering or terrorist financing concerning the information on the payer accompanying transfers of funds and corresponding records.

Data collection we mentioned in this question can't be used for other purposes. Of course Hungarian law for electronic communications also applies all rules for data processing due to Directive 2002/58/EC, e.g. provider could use electronic communications and consumer data for billing and marketing purposes.

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

According to Article 159/A of ECA a request could be made by the investigating authority (police), the public prosecutor, the court or the national security service. The purpose could only be to discharge their respective duties, which are defined by law.

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)?

The ECA itself does not contain exceptions. There is only a general reference in the ECA that responsibility for the legitimacy of such requests of information shall lie with the requesting party. The provider of electronic communications services transferring the data files shall be liable to ensure that the date retained and transferred are complete, of good quality and properly updated. Therefore the requesting party has to prove his legal position accessing retained data.

Electronic communications regulation does not contain such specific provision prohibiting retention of "sensitive communications data". Electronic communications providers shall apply general data protection rules in these cases, for example lawyer-client communication or doctor-patient communication.

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.

According to the Article 159/A Sec. 3 of ECA the period of retention is either one year or six months. The couse of the distinction is the type of the retained data.

Providers of electronic communications services, for the purposes of compliance with the obligation of disclosure following data for a period of one year following termination of the subscriber contract,

a) subscriber's name and address, place of abode, or registered office; if the subscriber is a natural person, the subscriber's birth name, and place and date of birth; if the subscriber is not a natural person, the subscriber's company number or other registration number, and the subscriber's bank account number related to fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these;

b) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, the telephone number allocated to the terminal equipment of the user or subscriber or to the subscriber access point, or the user ID or any technical identifier fixed in the subscriber contract or otherwise assigned to the subscriber or user by the provider of electronic communications services;

c) in connection with fixed network telephony services, fixed internet access services, or the combination of these, the address where the terminal equipment of the user or subscriber or the subscriber access point is installed, and the type of equipment.

Providers of electronic communications services, for the purposes of compliance with the obligation of disclosure following data for a period of one year following the time they were generated

a) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, the telephone numbers of the users and subscribers participating in the communication, their technical means of identification, user IDs, type of electronic communication services involved, and the data necessary to identify the date, time and duration of a communication;

b) in connection with fixed network telephony and mobile telephony services, or the combination of these, in cases involving call forwarding or call transfer, the subscriber or user number or numbers to which the call is routed;

c) in connection with mobile telephony services, concerning the equipment used at the time of communication, the International Mobile Equipment Identity (IMEI) of the calling and the called party, and the International Mobile Subscriber Identity (IMSI) of the calling and the called party;

d) in connection with mobile telephony services, the location label (cell ID) and network identifier at the start of the communication, and the data identifying the geographic location of cells by reference to their location labels (cell ID) during the period when Service was provided;

e) in connection with internet mail services and internet telephony services, or the combination of these, the data referred to in Paragraph d) of the intended recipient(s) of the communication;

f) in connection with internet access, internet mail services, internet telephony services, or the combination of these, type of the electronic communication service, the date and time of the log-in and log-off by the subscriber or, together with the IP address allocated to the communication, and the user ID of the subscriber or registered user, including the calling number;

g) in connection with internet access, internet mail services and internet telephony services, or the combination of these, the data necessary to trace any changes made in the unique identifiers of subscribers and users by the provider of electronic communications services (IP address, port number);

h) in the case of pre-paid anonymous mobile telephony services, the date and time of the initial activation of Service and the location label (cell ID) from which Service was activated.

Providers of electronic communications services, for the purposes of compliance with the obligation of disclosure shall retain data relating to unsuccessful call attempts for a period of six months following the time they were generated.

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)?

As mentioned in point 11 according to the ECA the bodies entiteled to access data are the police (investigating authority), the public prosecutor, the court and the national security service. And according to the DPA the data subject and the DP Commissioner also have the right to access this data.

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)?

As mentioned in point 12 the retained data could be used only to the purposes of the requester body's goals which are defined by law. These are for example law enforcement procedures, trials. Retained data could be also used in a civil action by the subject of the data.

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

According to Act CXXV of 1995 on the National Security Services these services are the following five authorities: Information Office (IH) and Constitutional Defense Office (AVH) as civilian, and the Military Information Office (KBH) and the Military Security Office (KFH) as military services. For technical support of the above mentioned four services there is the National Security Special Service. Their tasks are listed in the Act CXXV of 1995 as follows

"Article 4 The Information Office shall

a) obtain, analyse, evaluate and forward information of foreign relevance or foreign origin that can be used to promote the security of the nation, necessary for government-level decision making, and it shall pursue such activity as will promote the enforcement of the interests of the Republic of Hungary;

b) detect foreign secret service efforts and activities that violate or threaten the sovereignty, political, economic or other important interests of the Republic of Hungary;

c) collect information on foreign organised crime representing a threat to national security, in particular on terrorist organisations, on illicit drugs or weapons trafficking, illicit international trafficking of weapons of mass destruction and their parts, and the materials or instruments required for the manufacturing thereof;

d) detect foreign intents and acts that threaten the security of the economy and the financial status of the country;

e) take part in detecting and preventing the illicit trafficking of internationally controlled products and technologies;

f) safeguard Hungarian agencies (institutions) and establishments located abroad that are important for the activity of the administration;

g) carry out national security protection/control duties with regard to persons assigned to its competence;

h) provide specialist control, official authorisation and supervision of encryption, and produce encryption keys.

Article 5 Constitutional Security Office shall

a) detect and prevent foreign secret service efforts and acts which violate or threaten the sovereignty, political, economic, defence or other important interests of the Republic of Hungary;

b) detect and prevent covert efforts to alter/disturb the constitutional order of the Republic of Hungary by unlawful means;

c) repealed

d) detect and prevent covert endeavours which threaten the economic, scientific/technical, financial security of the Republic of Hungary, and illicit trafficking in narcotic drugs and weapons brokerage;

e) safeguard agencies (institutions) and establishments which are of importance for the activity of the central state power and the administration;

f) carry out national security protection/control duties with regard to persons assigned to its competence;

g) perform checks and related activities of persons requesting a permanent residence permit or, furthermore, refugee status or Hungarian citizenship, and — in connection with the protection of state sovereignty and constitutional order — of persons applying for a visa;

h) detect — until an investigation is ordered — crimes against the state (Criminal Code , Chapter X); crimes against humanity (Criminal Code , Chapter XI) and, in its field of operation, desertion abroad (Criminal Code , Art. 343); mutiny (Criminal Code , Art. 352), and endangering of combat readiness (Criminal Code , Art. 363);

i) repealed;

j) obtain information on criminal acts relating to violence against a member of a national, ethnic, racial or religious group (Criminal Code , Art.174/B); the violation of state secrets (Criminal Code , Art.221); causing public danger (Criminal Code , Art.259); the violation of an obligation based on international law (Criminal Code , Art.261/A); the seizure of aircraft (Criminal Code , Art.262); incitement against a community (Criminal Code , Art.269), and on scare-mongering (Criminal Code , Art.270);

k) take part in investigating, preventing, blocking the illicit traffic of internationally controlled products and technologies and in controlling their legal traffic;

l) take part in investigating, preventing, and blocking the illicit traffic of military instruments and services and in controlling their legal traffic;

m) upon the request of the National Security Supervisory Authority, it shall carry out industrial security inspections within its jurisdiction.

Article 6 The Military Intelligence Office shall

a) obtain, analyse and forward military policy, defence industrial and military information, of foreign relevance or origin, concerning the military element of security policy necessary for government-level decision-making;

b) reveal efforts directed against the Republic of Hungary indicative of offensive intent;

c) detect the efforts and activities of foreign military secret services that violate/threaten the sovereignty/defence interests of the Republic of Hungary;

d) collect information on illicit arms dealing representing a threat to national security and on terrorist organisations threatening the security of the armed forces;

e) take part in detecting and preventing the illicit traffic of internationally controlled products and technologies;

f) provide the pieces of information required for the strategic/operational planning activity of the General Staff of Defence;

g) safeguard Hungarian military agencies and establishments (institutions) located abroad which are of importance for the activity of the administration;

h) fulfil national security protection/control duties with regard to persons assigned to its competence.

Article 7 The Military Security Office shall

a) detect and prevent foreign secret service efforts and activities directed against the ministry headed by the minister responsible for defence and the Hungarian Army;

b) detect and prevent, in its area of operation, covert efforts to alter/disturb by unlawful means the constitutional order of the Republic of Hungary;

c) detect and prevent the efforts of foreign powers, persons or organisations to commit acts of terrorism against the organisations of the ministry headed by the minister responsible for defence and the Hungarian Army;

d) collect information regarding organised crime threatening the ministry headed by the minister responsible for defence and the Hungarian Army, in particular, especially, regarding illicit trafficking in drugs and arms dealing;

e) take part in detecting and preventing the illicit traffic of internationally controlled products and technologies and in controlling their legal traffic;

f) take part in detecting, preventing and blocking the illicit traffic of military technological instruments and services, and in controlling the legal traffic thereof ;

g) safeguard the designated government and military administration objects (institutions) within its jurisdiction;

h) carry out national security protection/control duties with regard to persons assigned to its competence;

i) detect, in its own area of operation, until an investigation is ordered, crimes against the state (Criminal Code , Chapter X); crimes against humanity (Criminal Code , Chapter XI); desertion abroad (Criminal Code , Art.343); mutiny (Criminal Code , Art.352) and endangering combat readiness (Criminal Code , Art.363),

j) detect acts of terrorism within its own area of operation (Criminal Code , Art.261);

k) obtain information on criminal acts involving violence against a member of a national, ethnic, racial or religious group (Criminal Code , Art.174/B); the violation of state secrets (Criminal Code , Art.221); the causing of public danger (Criminal Code , Art.259); the violation of a duty based on international law (Criminal Code , Art.261/A); the seizure of aircraft (Criminal Code , Art.262); incitement against a community (Criminal Code , Art.269), and scare-mongering (Criminal Code , Art.270); threatening with public danger (Criminal Code , Art.270/A); infringement of an obligation relating to the traffic of internationally controlled products and technologies (Criminal Code , Art.287), and detect every criminal act that threatens the execution of the constitutional functions of the ministry headed by the minister responsible for defence and of the Hungarian Army;

l) it shall carry out national security duties related to research, development, manufacturing and trade in defence pursued by the organisations of the ministry headed by the minister responsible for defence and of the Hungarian Army;

m) upon the request of the National Security Supervisory Authority, it shall carry out industrial security inspections within its scope of authority.

Article 8

(1) The Specialised National Security Service

a) shall provide services, upon written request, within the limits of the relevant legal regulations, with the special instruments and methods of intelligence information gathering and covert data acquisition, in support of organisations authorised to gather intelligence and acquire data covertly under the law;

b) as required by the organisations authorised under the law, shall provide the special technical instruments and materials needed for intelligence gathering and covert data acquisition activities;

c) shall establish special telecommunications connections for users specified by the Government;

d) shall provide official control with regard to the protection of security documents;

e) shall carry out expert activity;

f) shall carry out national security checks of persons assigned to its competence.

(2) The Specialised National Security Service may not be involved in government information provision activity.

(3) The Specialised National Security Service is a service providing organisation, which shall use the instruments and methods defined under Points a)-d), f) and g)of Paragraph (1) of Article 54 at its own discretion only to carry out its duties as defined under Point a) of Paragraph (1) and Point d) of Article 9.

(4) The Specialised National Security Service shall not use the instruments and methods of intelligence gathering as defined under Points e), h)-j) of Paragraph (1) of Article 54 and Article 56 at its own discretion except to carry out its duty defined under Point d) of Article 9. .

(5) The Specialised National Security Service shall provide services free of charge.

(6) The government shall determine the order of co-operation between the organisations authorised to gather intelligence information and acquire data covertly and the Specialised National Security Service."

In order to fulfil their tasks, the national security services may request data from any data management system, indicating the objective of requesting the data, and may have access to the systems and documents serving as basis for the records. The request for data shall be fulfilled also in respect of incomplete and fractional data. The fact of forwarding data shall be documented at both the delivering and the receiving organs. So there is no need to justify the request, it is enough to mention one of their task set forth in law.

Article 71 of the Criminal Procedure Code contains more general rules on these issue. The court, the prosecutor and the investigating authority may contact public bodies, business organisations, foundations, public endowments and public organisations to request the supply or transmission of information, data or documents, and may prescribe a time limit for fulfilling such request ranging between a minimum of eight and maximum of thirty days. Encrypted data and information made unrecognisable in any other manner shall be restored in their original condition by the supplier prior to communication or delivery, or made cognisable to the requestor thereof. Data supply shall be free of charge. Unless stipulated otherwise by law, the organization contacted shall fulfil the request within the prescribed deadline or state the reason for non-compliance therewith.

There are only a few garantees like requests concerning the provision of personal data shall only extend to the amount and type of data indispensable for the achievement of the objective of the request. The request shall precisely state the purpose of the data supply and scope of data required. If personal data coming to the notice of the requestor as a result of the request are not relevant for the achievement of the objective of the request, the data shall be deleted.

Practically there are no specific conditions for the data access.

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?**

    Regarding data retention rules of the ECA the entitled body can access retained data directly without any prior court permission and in this case the aggrieved party shall not be informed about the access.

    Regarding to the rules of criminal procedure code the court could order data retention on request of the public prosecutor or investigating body. The aggrieved party also shall not be informed about the access in this case.

    In Hungary regarding covered investigation rules public prosecutor or investigating body shall request the courts prior permission. Is it not required to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed.

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?**

    No notification needed and there is no deviation from this rule.

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

    According to the DPA the aggrieved party/data subject has the right to ask who and which purposes claimed access to his/her data. The service provider as main rule shall give a detailed answer to this request.

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

    Yes, according to DPA (Article 17-18) the aggrieved party/data subject has the right to turn to the court. The court shall order the controller to provide information about the retention, to correct or delete the data in question, or to honor the data subject's objection against retention. The court may also order publication of its decision. The aggrieved party also could claim for damages caused to him/her as a result of unlawful processing or by breaching the technical requirements of data protection.

    Special additional rules can be found in Government Decree No. 180/2004. (V. 26.) Korm. on the rules of cooperation between the organisations performing electronic communications tasks and the organisations authorised to collect confidential information and obtain confidential data.

In the case of breach of the obligations set forth in this Decree the provisions of Article 33 of ECA shall apply. The head of the organisation authorised to collect confidential information or of the electronic communications service provider may notify the President of the National Media- and Infocommunications Authority (NCA) on the breach of the obligations. If the confidentiality agreement is not concluded by the date and the cooperation agreement through fault of the electronic communications service provider the head of the organisation authorised to collect confidential information or the Director General of the National Security Service shall notify thereof the NCA President. If the electronic communications service provider fails to fulfil the decisions adopted by the NCA President in its resolution closing the coordination procedure the Authority will take action against it according to paragraph (1).

There is also a specific rule on liability in Article 20 of the Decree. In the proceedings instituted against the electronic communications service provider due to infringement of rights connected with personal data the organisation authorised to collect confidential information will be liable only exclusively according to the applicable laws – even when the electronic communications service provider has not committed a fault.

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, according to the subparagraph (4) of 159/A of ECA, the provider transferring the data shall be liable to ensure that the data retained and transferred are complete, of good quality and properly updated. According to the DPA (Article 10) providers as data processors must implement adequate safeguards and appropriate technical and organizational measures to protect data, as well as adequate procedural rules

And according to the subparagraph (5) of 159/A of ECA, providers could only be authorized to subcontract their data processing operations, or to store the data retained in another Member State of the European Economic Area, if the agreement for the retention of data concluded with the data processing contractor contains provisions laying down the requirements for security and access in due compliance with Hungarian regulations concerning secrecy and the protection of classified information. So outside the EEA countries it is not possible to retain or store data.

According to Government Decree No. 180/2004 the electronic communications service provider shall ensure exclusion of illegal access to the technical system, the data stored therein and the other apparatus used for collection of confidential information.

And according to Article 2 of the Government Decree No. 226/2003. on the Special Conditions of Data Management by Electronic Communications Service Providers, the Data Security of Electronic Communications Services, and the Rules of Identifier Presentation and Call Diversion service provider shall select and operate

the electronic communications devices used for the management of personal data during the provision of Service in such a way that

a) the managed data are available to the authorized persons (availability),

b) the authenticity and authentication of the managed data are ensured (authenticity of data management),

c) the consistency of the managed data can be proven (data integrity),

d) the managed data are protected against unauthorized access (confidentiality of data).

Service provider shall ensure the protection of the security of data management with technical and organizational measures that provide a level of protection corresponding to the risks arising in connection with data management."

Moreover in Article 3 Service provider shall draw up a data protection and data security code on the detailed rules of the management of personal data, the selection and operation of devices used for the management of personal data,as well as of data transmission and record-keeping associated therewith .

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

As mentioned in point 13 the time limit for data retention is either 1 year or 6 months. If there is no request for access, the provider shall delete data immediately after this period is over (according to DPA's principle: after processing is not longer necessary data shall be deleted). Accessing bodies have the similar obligation: after the processing is not longer necessary (the procedure is over for good, so when there is no more appeals possible) they have to delete the data due to Article 14 Sec. 2. Point d) of the DPA .

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.

Due to Article 159/A Sec. 1 electronic communications network operators and providers of electronic communications service obliged to retain generated or processed data. Two groups of providers will be defined as follows.

Electronic communications network operator shall mean a natural or legal person or unincorporated business association providing or authorized to provide, a public electronic communications network or an associated facility (Art. 188 Sec. 20 ECA). These group of providers is in praxis easily to identify.

Provider of electronic communications services shall mean the operator of an electronic communications network and any natural or legal person or

unincorporated business association engaged in providing electronic communications services (Art. 188 Sec. 14 ECA). To indentify these group we have to apply the term for electronic communication services (Art. 188. Sec. 13 ECA), which means

a) a service normally provided for remuneration which consists wholly or mainly in the conveyance and, where applicable, switching or routing of signals on electronic communications networks,

b) but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and electronic communications services;

c) furthermore, it does not include information society services, as defined in specific other legislation, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

In the praxis those electronic service providers are obliged to data retention, which transmit (switch or route) signals on electronic communications networks, but conent providers are excluded from that obligation. No other providers are obliged to retain data.

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

There is no exemption neither by law or by request.

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

The ECA was excepted in 2003 and came on 1st of January 2004 into force, the rules on data retention were amended in 2007, which came on 15th of March 2008 into force. The 2003 regime of data retention contained the following categories of data:

- until the termination of the subscribers contract -

subscriber's name and address, place of abode, or registered office;

if the subscriber is a natural person, the subscriber’s birth name, his/her mother’s name and place and date of birth;

if the subscriber is not a natural person, the subscriber's company number or other registration number, and the subscriber's bank account number;

- for three years from their generation or procession -

numbers to which the call is routed;

direction of a call or other service, date;

time and duration of a communication;

amount of transmitted data;

in connection with mobile telephony services cell ID and network identifier;

in connection with mobile telephony services, IMEI and in case of IP networks applied identifiers

date of call or service

data connected with the payment of charges or charges in arrears;

events of the termination of a subscriber contract if terminated with debts outstanding;

data relating to other, non-electronic communications services, in particular to the billing of charges therefore, that may be used by subscribers and users in the case of telephone services.

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)?

No, general rules apply (Government's decree 180/2004 and Government's decree 226/2003)

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)?

According to the existing rules all the costs which originate from the implementation of the directive are borne by the providers. These are mostly the costs of the technical devices, the cost of the solution of connection and interoperability of these devices, and also costs of the technical staff (Article 7 of Government Decree 180/2004).

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

    There is no possibility to reimburse for the costs of the providers.

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

    Any investigating authority, public prosecutor, courts or the national security service can request retained communication data, where these bodies has to give grounds of the request, for the legitimate ground is the requesting party liable. The provider of electronic communications services transferring the data files shall be liable to ensure that the date retained and transferred are complete, of good quality and properly updated. There is no detailed rule for providers which aspects can be considered by fulfilling a request, or in what cases shall they deny it.

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.**

    There is no specific rule for this cases. In case of any damage general rules of the Civil Code apply.

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?**

    For the entitled bodies is a direct access through a request secured.

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?**

    There aren't regional entities.

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?**

In the course of the Directive's transposition there were no general rules on co-operation adapted.

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)?**

Between the Member States the exchange of retained data is possible in the frames of the Cybercrime Convention, although there are several legal aid treaties with other Member States. Foreign state bodies cannot access retained data directly.

As an example for legal aid treaties we have to mention agreements on enhancing cooperation in preventing and combating crime. Hungary made such agreements for with Romania, Bulgaria, Croatia, Serbia and with the USA.

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

The Data Protection Authority is in charge of monitoring on his general competence in this field. The institution of the Data Protection Commissioner is independent from the government, other state organisations and the private sector; he cannot accept orders from them. His competency covers both state and private sectors, and he is responsible for reporting his activity to the Parliament only.

His decision and statements can be challenged before the court. The Hungarian DPA is leading technical and legal investigations. His main tasks are moreover supervision of data controlling, keeping the Data Protection Register, proposing legislation, amendment of laws, supervision of justification of the scope of state and official secrets, promoting the culture and knowledge of fundamental rights.

The Data Protection Authority have the right to monitor compliance of the operators/providers with data retention obligations. Article 29 Working Party made

such general investigations reviewing the data retention implementations, where the Hungarian DPA also participated.

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 we mentioned at point 1. there is a pending case Nr. 568/B/2008 before the Constitutional Court of Hungary in connection with this transposition.

If so, please answer to the following questions:

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

Plaintiff is the Hungarian Civil Liberties Union (TASZ), but due to it's abstract nature in cases before the Constitutional Court of Hungary there are no defendants/respondents.

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

The constitutional claim of the HCLU challenges the whole Amendment of ECA regarding data retention. The plaintiff's main concern in its complaint was the retention of personal data for 'the stock' without previously defined purposes. Such data processing has been prohibited by a 1991 decision of the Constitutional Court. The Act on Protection of Personal Data (1992), also contains this ban. HCLU has stressed that data retention might be detrimental not only to privacy but also to other fundamental rights such as freedom of information, freedom of the press, freedom of conscience, freedom of religion, freedom of assembly and freedom of petition.

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?

Constitutional Court of Hungary didn't decided in the case and the Court has no power to issue a temporary order.

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)?

There are no lawsuits with European courts.

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 Service providers' premises, with external companies, with the State)? Are the data stored locally or at a centralised level?

In Hungary there are no centralised structures to store retained data. Providers storing data locally, but the main providers store them at there seat central. There is also known a solution where the provider stores retained data in a separated database to fulfil their obligations towards entitled bodies. Physically providers store retained data inside of Hungary because of technical reasons.

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?

Providers of electronic communications services subject to the obligation of retention are authorized to subcontract their data processing operations, or to store the data retained in another Member State of the European Economic Area, if the agreement for the retention of data concluded with the data processing contractor contains provisions laying down the requirements for security and access in due compliance with Hungarian confidentiality regulations concerning the data requests. Providers of electronic communications services are not authorized to store any data retained in the territory of a country, and may not contract Services of a data processing contractor that is established in a country, which country is other than a Member State of the European Economic Area. In case of storing outside of Hungary national data protection law shall be applied.

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

a) no data are retained beyond what is permitted?

As mentioned in point 12 according Article 159/A Section 4 ECA the requester is responsible for the legitimacy of the requests. Providers have to secure technical measures: according to DPA principles. Data processing with various aims shall be separated or access rules has to be detailed enough.

This principle emerge in Article 2 of the decree 226 of 2003. According to this the provider shall select and operate the electronic communications devices used for the management of personal data during the provision of Service in such a way that

a) the managed data are available to the authorized persons (availability),

b) the authenticity and authentication of the managed data are ensured (authenticity of data management),

c) the consistency of the managed data can be proven (data integrity),

d) the managed data are protected against unauthorized access (confidentiality of data).

Service provider shall ensure the protection of the security of data management with technical and organizational measures that provide a level of protection corresponding to the risks arising in connection with data management. Service provider shall draw up a data protection and data security code on the detailed rules of the management of personal data, the selection and operation of devices used for the management of personal data,as well as of data transmission and record-keeping associated therewith .

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)?

In Hungary due to Government Decree No. 180/2004. on the rules of cooperation between the organisations performing electronic communications tasks and the organisations authorised to collect confidential information and obtain confidential data only the National Security Agency has the right to use technical interfaces directly connected with electronic communications.

On the other hand due to Article 92 ECA providers are required to cooperate with organizations authorized under specific other legislation by another act to conduct covert investigations and covert information gathering operations. Providers shall operate facilities in their electronic communications systems so as not to prevent or block covert investigations and covert information gathering operations. Providers are required to inform the National Security Agency directly, concerning any activities, services, products, or any changes therein. They also can be required to install the technical means necessary to comply with the requirements, such as a basic monitoring subsystem, with access terminated at the exit point, for the National Security Agency within six months from the date of receipt of notice concerning the basic requirements in terms of technical means. All costs for the installation of a basic monitoring subsystem shall be borne by the service provider.

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

There are no such technical or organisational measures prescribed by law, just the principle: data could used only for that purposes they are permitted to be used, every other usage is unlawful.

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.

Providers are liable for data security, which obligation has to be fulfilled in consideration with general data protection legislation. Providers, as data controllers ensure data security and shall take all technical and organisational measures and elaborate the rules of procedure necessary to enforce compliance with this Act and other rules pertaining to data protection and confidentiality.

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

There are no such technical or organisational measures prescribed by law, just the principle: data could used only for that time till they are permitted to be used, every other usage is unlawful.

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)?**

Notification doesn't needed according to the law.

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

There are no such technical or organisational measures prescribed by law, just the principle: data could used only for that purposes they are permitted to be used, every other usage is unlawful.

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)?**

Regarding to Article 31/A of the Hungarian DP and FOI Act an internal data protection officer shall be appointed or commissioned within the organisation of the data controller or of the technical data processor.

The internal data protection officer shall

a) contribute to or assist in making decisions related to data processing and to the enforcement of the rights of data subjects;

b) monitor compliance with this Act and other rules of law on data processing, as well as with the provisions of internal data protection and data security rules and with data security requirements;

c) investigate reports submitted to him, and call on the data controller or technical data processor to discontinue any unlawful data processing observed by him;

d) draw up the internal data protection and data security rules;

e) maintain the internal data protection register; and

f) ensure the training of the staff in data protection.

According to ECA and data protection legistlation providers has to appoint an internal data protection officer holding a higher education degree in law, public administration or information technology, or a qualification equivalent thereto within the organisation of the provider or his data processor and he shall report directly to the provider. There are also internal controlling systems and data protection auditors on the Hungarian market.

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?

According to Article 2 of the decree 226 of 2003 The provider shall select and operate the electronic communications devices used for the

management of personal data during the provision of Service in such a way that

a) the managed data are available to the authorized persons (availability),

b) the authenticity and authentication of the managed data are ensured (authenticity of data management),

c) the consistency of the managed data can be proven (data integrity),

d) the managed data are protected against unauthorized access (confidentiality of data).

Service provider shall ensure the protection of the security of data management with technical and organizational measures that provide a level of protection corresponding to the risks arising in connection with data management."

As mentioned before, it is the providers choise and liability to find and to use the best and most secure solution. Also the provider is liable for the interoperability of the choosen solution.

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.

Co-operation between the party retaining the data and the party accessing them effected in practice goes on case by case without any agreement. The National Security Agency is an exception because of their special rights and privileges.

The entitled party has to send an official request to the retaining party or asking the National Security Agency to start the request procedure due to Government Decree No. 180/2004. (V. 26.) on the rules of cooperation between the organisations

performing electronic communications tasks and the organisations authorised to collect confidential information and obtain confidential data

Organisations authorised to collect confidential information may request the conclusion of a written cooperation agreement to set forth the detailed rules applicable to the performance of the tasks. When requested, the electronic communications service providers shall conclude the agreement within 60 days of the request.

The agreement to be concluded with the National Security Service shall include the following:

a) the method and rules of making a request of data which may be disclosed through collection of confidential information subject to permits identified in other law, and of the fulfilment of such request;

b) the levels and method of keeping contact;

c) the method and rules of requesting and ensuring what is identified;

d) the rules of the notification and coordination procedure connected with electronic communications network and service development and the establishment and development of the system;

e) the number and location of the entry points to be provided by the electronic communications service provider;

f) the method of application of the rules of protection of data and privacy and the method of protecting the technical apparatus and solutions;

g) the rules of selecting, coordinating and controlling the employees participating on behalf of the electronic communications service provider;

h) the rules of fulfilment, and evaluation and revision from time to time of the cooperation agreement;

i) the rules of data supply;

j) the method of satisfying claims of reimbursement of costs and other compensation, the rules of settlement; and

k) any other condition and procedure in addition to sub-paragraphs a) to j) which the cooperating parties consider necessary to be set forth in writing.

Should be parties fail to reach an agreement on any cooperation matter either of them may request the President of the National Communications and Media Authority to conduct a coordination procedure.

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?

The cross-border issues are delt by either international standards or by EU rules. For example in the field of criminal procedures by EU member states the common rules are followed. Due to Act 130 of 20023 on cooperation in criminal procedures with EU Member States Hungarian authorities can offer a legal aid in form of direct notification, undercover gathering of information with or without judicial permit. These activities of Hungarian authorities underlying regular control by the prosecutor.

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).

There was no general and broad debate on introducing data retention. There were several counterarguments in the parliamentary debate because the lack of financial compensation for the providers and there was also a proposal to the draft aiming shorter retaining periods, but there were not accepted. Some civil groups like human rights organisations and the obliged providers argued against the harmonisation, but there was no political party or pressure group to represent these interest. At this time the Hungarian DPA examines relation between the Directive and the effective harmonisation. During the examinations the Hungarian DPA will pay attention to legislation and current status data retention rules of other Member States. There is no result of this assessment yet.

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)?

There are several other legal obligations to retain data like PNR, employment data, financial transactions or social security but processing of personal data can only done with specific and appropriate purpose. In every Hungarian legal act the processing of personal data could only be prescribed with a specific reason. In the case of PNR the specific reason to retain data is the protection of passengers and security of flight service and this reason makes the retention legally acceptable.

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.

There is statistics or research result available on the topic and as it was mentioned the proper harmonisation of Article 10. Data Retention Directive failed, because there is no selected authority to transmit data for the Commission.

It has to be mentioned that the Hungarian Civil Liberties Union requested statistical data from the police, public prosecutor and from the national security agency. Only the General Public Prosecutor provided detail information. Hungarian Civil Liberties Union also brought an action against the National Security Agency to publish statistical data on accessing retained communications data. The case is still pending.

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 aren't any available information.

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?

It is expected to have an intensive discussion in 2011 generally on data protection issues and data retention as one of the topics. The Hungarian DPA signalized more general investigation on data retention.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications:

Which data are – according to national (constitutional) law1 – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

There are several fundamental rights in the Constitution of Hungary which protect secrecy of communications. Human dignity as general right to personality protection covers all fundamental rights on communication, but protection of privacy and personal information (Article 59) gives the concrete constitutional basis for protection. Secrecy or confidentiality of communication is not a fundamental right and it is not part of the Constitutional Courts jurisdiction, the right to privacy and human dignity cover these fundamental interests. Data retention can affect other fundamental rights and principles indirectly, like freedom of speech combined with freedom of religion and freedom of press, but judiciary basic rights too. The Hungarian constitutional jurisdiction is neither protecting freedom of thought or freedom of profession in cases where the confidentiality of communication is essential. These fundamental principles are covered by fundamental rights mentioned before. Source of these right are directly the Constition, although several legal position are based on Acts like client-lawyer communication or patient – doctor communication.

Due to jurisprudence of the Hungarian Constitutional Court according to Art. 59 of the Constitution everybody is entitled in the Republic of Hungary to the right to good reputation, to the inviolability of private premises as well as to the protection of private secrets and personal data. The right to the protection of personal data, as guaranteed by Art. 59 of the Constitution, means that everybody is free to decide about the disclosure and use of his own personal data. Hence, approval by the person concerned is generally required to register and use personal data; the entire route of data processing and handling shall be made accessible to everybody, i.e. everybody has to right to know who, when, where and for what purpose uses his data. In exceptional cases, an Act of Parliament may order the compulsory supply of personal data and may also prescribe the way these data may be used. Such an Act of Parliament restricts, the fundamental right of informational self-determination, and it is constitutional only if it is in accordance with the conditions specified in Art. 8 of the Constitution. Any legal rule which, irrespective of the procedure to be adopted, provides for the taking, collecting, storing, handling, forwarding, publicizing, altering, preventing further use, producing new information or on any other use of personal data shall be in conformity with Art. 59 of the Constitution if it comprises guarantees that the person concerned is able to monitor the route of his data during the processing and to enforce his rights. The legal institutions for this purpose, therefore, have to secure the concerned party's approval to the processing and have to contain specific guarantees for those special cases when data processing may take place without the approval of the person concerned (possibly without his being aware of it).

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

These legal institutions in charge of these guarantees for the purposes of verification have to contain the route of the data within objective limits. Adherence to the goal to be achieved is a condition of and at the same time the most important guarantee for exercising the right to informational self-determination. This means that personal data may only be processed for a definite and legally justified purpose. Every single stage of the data processing shall conform to the declared and authentically set objective.

The person concerned shall be informed of the purpose of the data processing in such a way so as to enable him to judge the effect of data processing on his rights, and to make a well-founded decision on the provision of his data; furthermore, to allow him to enforce his rights if the use of his data deviates from the original purpose. For the same reason, the person concerned shall be notified about any possible change in the purpose of the data processing. Processing with a new purpose is legal without the concerned person's approval only if it is expressly permitted by an Act of Parliament with respect to the data in question and to the processor. It follows from the principle of adherence to the goal to be achieved that collecting and storing data without a specific goal, "for the purpose of storage", for an unspecified future use are unconstitutional.

The other basic guarantee is the restriction on the forwarding and publication of data. Data forwarding, in the strictest sense, means that the data processor makes the data accessible to a certain third party. Publication of the data means that any third person can have access to the data. Those, usually professionals, who are entrusted by the data processor to perform the physical or the computer-related activity of data processing are not considered "data processors", and their access to the data does not constitute "data forwarding". The responsibility of such a party can be regulated separately, without affecting the data processor's full responsibility with regard to its own data processing activity or that entrusted to somebody else by the data processor.

Personal data may be made accessible to a third party, other than the concerned party and the original data processor, and thereby to link up data processing systems, only if all the conditions required for data forwarding as related to each item of data are fulfilled. This, therefore, may mean that the recipient of the data forwarding activity (the one who requests the data) shall either have a specific authorization by an Act of Parliament to process the forwarded data, or it shall have approval by the concerned party.

Adherence to the goal to be achieved is, of course, the major impediment to data forwarding. The requirement of adherence to the goal to be achieved, and the above specified conditions of change in the goal to be achieved and data forwarding also impedes the flow of data within and among state administrative organs.

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

The Constitutional Court has a various competence to examine constitutionality of Hungarian legal rules, although his procedure have an abstract nature dealing only with the given legal rule not with the merit of the case. In case of personal data the Court applies the necessity – proportionality examination (basic test for fundamental rights), but in case of necessity constitutionality of legal basis (consent or legal rule) will be examined, on the other hand examination focus on purpose binding data processing.

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

There is a pending case before the Constitutional Court and there is no public information on status of the procedure.

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?

There is no absolute limit to which public surveillance measures collectively may restrict privacy, constitutional jurisprudence examines the balance of interest in each case. Basically surveillance or data retention or any method of data processing has to be based on consent or legal rule and the proportionality of the fundamental right's restriction is measured by fulfilling of data processing purpose bound nature. From that point of view the absolute limit is the fundamental right's restriction.

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)?

There is no exemption for the providers.

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?

Providers fundamental right's to enterprise and the right to property is limited by data retention legislation. These issues were only debated besides privacy issues and didn't got too much attention. In our personal opinion right to enterprise is not limited because data retention means only another sector specific imposition and therefore won't have a huge impact on the undertakings. Due to constitutional jurisprudence lack of compensation for the providers can be classified as unproportional limitation, because data retention belongs to the state's task and therefore the cost shall bear by the state. Due to our assessment these cost (infrastructure, manpower, management) are unproportionally high to the obtained goal.

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)?

From the providers point of view involving them into the data retention operation in itself doesn't raise constitutional concerns. Moreover the missing possibilities for reimbursement and inadequate procedural legislation can lead much more to abolishment of the give regulation by the Constitutional Court.

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

There is no legal ground to claim for reimbursement.

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 and, in particular ECHR has the same status as a Hungarian act or other legislation. From the constitutional point of view there is a difference due to Article 43-47 Act on Constitutional Court, because the Constitutional Court examines laws or other legal means of state administration for conflicts with international treaties ex officio or upon the petition of specified organs and persons If the Constitutional Court establishes that a law or an other legal mean of state

administration at the same or lower level than the law promulgating the international treaty conflict with the international treaty, it annuls in whole or in part the law or the other legal mean of state administration contrary to the international treaty.

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?

To the transposition of a Directive it shall an act on harmonisation to be passed. Hungary has a dual system regarding national and international law, although jurisprudence of the European Court of Justice overrule this rigid separation.

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?

Due to Article 2/A of the Hungarian Constitution Republic of Hungary may, in order of her participation in the European Union as a member state, based upon international treaty, exercise certain constitutional competences, to the extent that is necessary to exercise rights and perform obligations, under the European Communities and European Union foundation treaties in conjunction with the other member states; the exercise of these competences may be realized independently, through the institutions of the European Union. A majority of two-thirds of the votes of the Members of Parliament is required for the ratification and adoption of the international treaty specified in paragraph. .

It means that there is no general constitutional rule on transferring national sovereignty, with the 2/3 constitutional majority the Parliament can unlimited transfer any competencies.

There is no decision of the Constitutional Court on conflict between constitutional law and community 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?

DPA and National Communications & Media Angecy has competences regarding data protection, there aren't any regionals authorities.

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

Constitutional law have'nt set any limit, but the DPA contains such a rule on transmission of data to third countries.

Section 9.

(1) Personal data (including special data) may be transferred - irrespective of the medium and the manner in which it is transferred - to a third-country controller or processor if:

a) the data subject has given his consent; or

b) the transfer is permitted by law and the laws of the third country in question afford an adequate level of protection with respect to the processing of the personal data transferred.

(2) Adequate level of protection of personal data is deemed available if:

a) the Commission of the European Communities has determined - under a legal act contained in specific other legislation - that the third country in question ensures adequate level of protection;

b) there is a treaty between the third country and the Republic of Hungary containing guarantees for the rights of data subjects referred to in Section 11, their rights to remedies, and for the independent control of data management and data processing operations;

c) third country controller or processor offers appropriate safeguards to ensure adequate level of protection in the course of data management and processing personal data, the basic freedoms and rights of data subjects, in particular, if data management and processing is carried out in compliance with the legal act adopted by the Commission of the European Union contained in specific other legislation.

(3) Personal data may be transferred to third countries within the framework of an international agreement for mutual legal assistance, for the purpose and with the contents specified in the agreement.

(4) Transmission of data to EEA Member States shall be treated as if the transmission took place within the territory of the Republic of Hungary.

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 excepted that the Constitutional Court brings a decision in 2011 and in case of the annulations a wide social debate could start on data retention and generally on privacy. On the other hand the Hungarian DPA already signalized that besides social networks one of the main topic will be data retention. It can lead to amendment of the given legislation and more social awareness.

There is a clear need for modification of Hungarian data retention regulation. According to our opinion there are two motivating factors which can lead to a quick change. On the one hand the Constitutional Court can declare the data retention rules null and void, and therefore this decision could lead to modification. Or on the other hand an infringement procedure by the European Commission because of ineffective harmonisation could lead us to change the law.

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

Hungary

Dr. Géza Tényi LL.M.

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*?

There is no subjective right to communicate anonymously, although there are just a few prohibitive rules for using PETs.

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?

As we mentioned in the first Questionnaire Part 1. A. I. 2. there was no national authorities responsible for providing yearly based statistics to the Commission regarding Article 10. Hungarian regulation was amended on the 19th July 2011. Now the regulation is similar to the Directive regarding the statistical data transfer to the Commission. This amendment come into force on 3rd August 2011.

There is no actual debate on this topic, neither on improvement nor on quick-freeze.

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?**

   Generally private actors are obliged to cooperate with public authorities in every official cases and investigation regarding criminal offences, or public administration cases and civil cases as well. There are only several exceptions when the obligated person can refuse cooperation, i.e. business secrets, prohibition of self-accusation.

   There are different business sectors in which providers are obligated to retain data, i.e. financial services, medical services or by every tax transaction.

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?**

   Due to procedural regulations as Criminal Procedure Code or Civil Procedure Code, even due to Procedure Code on administrative cases a person, even a relative can refuse to testify or to deliver evidence against themselves or their relatives. A person who is obliged to confidentiality because of his or her profession as lawyer, doctor and priest, eventually every public officer can also refuse to testify of to deliver evidence if he or she won't get a permission to do that.

   Because of their general wording these rules include also data which has to be retained.

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?**

   There are no specific rules for storing retained data by entitled bodies, however they have to fulfil general data protection rules including data security measures.

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.**

   As we mentioned at Question 2. from the 3rd August 2011 some public bodies - as courts, prosecutors, security services and police are obliged to send official statistics

on transmission of retained data for the Commission. There are no specific rules on the availability of these statistics by the public.

B. Country-specific questions

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

Data retention regime as a whole is in our opinion unconstitutional, because it means a data collection without definite purpose and for arbitrary future use.

Regarding the central decision of the Constitutional Court from 1991 in the absence of a definite purpose and for arbitrary future use, the collection and processing of personal data is unconstitutional. The right to the protection of personal data, known as the right to informational self-determination, as guaranteed under Article 59 of the Constitution, permits everyone the freedom to decide about the disclosure and use of their personal data to the extent that the approval of the person concerned is generally required to register and use it. In addition Article 59 of the Constitution ensures that such person can monitor the entire route of data processing thereby guaranteeing the right to know who used the data and when, where and for what purpose it was used. A statute could exceptionally require the compulsory supply of personal data and prescribe the manner of its use provided it complied with Article 8 of the Constitution.

Moreover we have concerns if data retention even fit the necessity-proportionity tests of the CC, not to mention that it is not confirmed as an appropriate instrument of crime-prevention.

Therefore we accept that the Constitutional Court will abolish data retention regulation as a whole. You can find the given decision @

http://www.mkab.hu/admin/data/file/738_15_1991.pdf

8. With the adoption of the new Constitution, due to enter into force 1 January 2012, the fundamental rights system and other constitutional provisions explained in your answers to questions 50 to 62 of the first questionnaire might have changed. Could you update your answers in this regard?

The new Constitution won't affect the core of fundamental rights, especially the protection of personal data, communication rights or any other privacy. Due to the new constitutional order these fundamental rights shall be detailed in the so called "cornerstone acts" with 2/3 majority. These acts will be accepted in the forthcoming months. Therefore our answers don't need to be updated.

Reportedly, the new Constitution also limits the competence of the Constitutional Court to check the compliance of national laws with the Constitution. Does this change affect in any way the laws enacted to transpose the Directive or any amendments to be enacted in the future?

The competences of the Constitutional Court have been changed, definitely, but in a different way. Until now the main competence of the CC was the preliminary general abstract norm control, which will be cut down to a special group of initiators. Secondly, the competence of the CC regarding budgetary issues will be limited for special cases as infringement of human dignity, data protection, freedom of speech and freedom of belief. Therefore the limitation of competencies does not affect protection of personal data.

These changes does not affect the transposition of the Directive or any amendments.

9. **Do you have any news on the case Nr. 568/B/2008 before the Constitutional Court of Hungary, mentioned in your answer to questions 1 and 36? If the court has already ruled on this case: does it provide any specific elements that have to be considered or certain aspects that have to be balanced against each other when assessing whether or not the national law transposing the Directive is in line with the Constitution and other overriding law?**

   The CC has not been decided yet, it is still a pending case.

10. **As regards your answer to question 17 of the first questionnaire: could you please clarify which bodies need to seek a court order prior to requesting retained data from an obligated party (provider), and which do not. Please also specify the legal norms where this is laid down. Please describe the steps the entitled body has to take in order to obtain a court order prior to the data request. What will the court examine before taking a decision on whether or not to issue the order? Which cases are to be regarded as "emergency cases" so that access to the data may be sought by the Prosecutor or the Investigating Judge? Is it necessary to have a court decide on the lawfulness of the access after the emergency situation is over?**

    As we mentioned it by question 17 in the first Questionnaire, due to the Criminal Procedural Code in combination with the Act on Police and with the Act on National Security Services only in the case of covered investigation shall the requester have a prior court order, police and national security in the given case. A covered investigation could include data retention measures, but even much more harder arrangements i.e. as wire-trapping. That is the reason of a court order. For a „simple" data retention request a court order doesn't needed.

    Article 202 Section 6 of Criminal Procedure Code contains the conditions when covered investigation can be ruled by a court order. Covert data gathering may only be conducted if obtaining evidence by other means reasonably appear to be unlikely to succeed if tried or would involve unreasonable difficulties, and there is probable cause to believe that evidence can be obtained by covert data gathering.

    Due to Article 201 Sec. 1. of the Criminal Procedure Code covert data gathering may be applied if the proceedings are conducted upon the suspicion of a criminal offence, or an attempt of or preparations for a criminal offence which

a) has been committed intentionally and punishable by five years' or more imprisonment,

b) is related to trans-boundary crime,

c) has been committed to the injury of a minor,

d) has been committed repeatedly or in an organised manner (including criminal offences committed for profit, in a criminal organisation and conspiracy),

e) is related to narcotics or substances qualifying as such,

f) is related to counterfeiting of money or securities,

g) has been committed with a weapon.

(2) If the investigation is conducted by the prosecutor [Section 28 (4) e), Section 29, Section 474 (2)–(4)], covert data gathering may also be performed in the case of criminal offences not listed in subsection (1).

Due to Article 203. Sec. 6 of the Criminal Procedure Code if the permission procedure caused a delay that would jeopardise the success of covert data gathering, the prosecutor may, for maximum period of seventy-two hours, order covert data gathering (exigent order). In this case, simultaneously with the order, the motion for the permit shall also be submitted. If the court has rejected the motion, a new exigent order may not be issued based upon the same facts.

11. **As regards your answer to question 9 of the first questionnaire: What considerations during the legislative procedure have led to the deviations between the Directive and the national law in terms of the data categories to be retained (more detailed information to be retained under the national law, compared to the Directive)?**

    There are no public information on these considerations.

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

    There are no rules against duplication of data, every provider has to retain data without considering of any other retention.

13. **Are there any specifications regarding data security with respect to storage and transmission (objectives to be achieved – e.g. "adequate confidentiality" – and/or quality requirements to be fulfilled – e.g. an obligation to encrypt the data before transmitting them to the authorised bodies)? If so:**

    There are no specific rules for that case, general data security rules apply. In the new data protection act from 2012 there will be more changes on that topic.

14. **Are the technical and organisational measures necessary to implement the legal requirements on data protection and data security (e.g. Art. 2 of Decree 226 of 2003, as mentioned in your answer to question 40 a) of the first questionnaire) standardised or specified any further, e.g. through guidelines issued by the supervisory authority? If so: Are these specifications binding or not for the bodies concerned? Please describe their content.**

    In particular: do they provide for measures in one or more of the following areas:
    - physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)
    - secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)
    - rules on internal access restriction and control (e.g. four-eyes principle, secure authentication mechanisms/certificates)
    - access logging
    - secure (irreversible) deletion after expiry
    - error correction mechanisms (e.g. hash functions, checksums)
    - secure data transmission (cryptographic security, postal delivery)
    - access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)
    - measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)
    - staff training/internal control mechanisms to ensure compliance with the law and other rules
    - measures to ensure that the principles of data reduction and data economy are respected (e.g. rules that avoid double retention of data by both the service provider and the operator of the network used for signal conveyance)

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

    There are no such rules yet, neither the DPA nor the NRA has adopted any guidelines.

15. **As regards your answer to question 43 of the first questionnaire: are you aware of any such agreement to have been concluded with the National Security Service? If so, please specify the company/companies having done so and – as far as this information is available to you – the concrete content.**

    As these kind of agreements were concluded with the National Security Service, therefore their content is a state secret.

16. **Please describe the rules governing the exchange of data among public authorities in general, as far as they apply also to data retained under the national laws transposing the Directive. Are there any provisions that allow the bodies entitled to obtain access to the data retained to transfer these data, once**

obtained, to other authorities for their respective purposes? If so, please describe the requirements that have to be fulfilled for such transfer, and how data exchange between them is effected in practice.

There are no specific rules how public authorities can exchange retained telecommunication data. Procedural codes for civil, criminal and administrative procedure make it possible for public authorities to cooperate with each other and eventually they have to fulfil general data protection rules within their cooperation.

17. **As regards your answer to questions 34 and 44 of the first questionnaire: which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)? Which national legal norm is such data exchange based upon?**

    Courts, prosecutors, police and secret service bodies are entitled and responsible to serve cross border data exchange request. The Criminal Procedural Code and Secret Services Acts are the core of their activities, which are complemented by international treaties and legal assistance charters.

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

    Public prosecutors supervising the activities of the police, generally the DPA have the duty to supervise any data processing activity in Hungary. Both are independent in the sense of the Directive.