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

The Czech Republic

Moreno Vlk & Asociados – JUDr. Václav Vlk, attorney at law

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

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

I. Legal provisions

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

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

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

The Directive 2006/24/EC (hereinafter only „the Directive") was transposed into the national law of the Czech Republic in 2008 by the Act. No. 247/2008 Coll. which has modified the Act No. 127/2005 Coll., on electronic communications (hereinafter only „Electronic Communications Act"). However, a previous text of the Electronic Communications Act which was published on 31 March 2005 and came into efect on 1 May 2005 has already taken into account the Directive, which was being prepared in that time. Therefore, tha majority of the rules stipulated by

the Directive were at the date of the Directive"s effectiveness already transposed to the Czech legal system. Therefore, the Act. No. 247/2008 Coll. only modified the Electronic Communications Act and specified more precisely some stipulations and definitions (for example determined newly an obligation of retention the data concerning "unsuccessful call attempt").

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

2. **What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?**

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

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 accomplished:*

General questions

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

   A text of the Electronic communication act as it was approved in 2005 may be found at:

   http://aplikace.mvcr.cz/archiv2008/micr/files/1282/electronic_communications_act.pdf.

   However, this text is not effective in total actually, all consequent modifications must be taken into consideration. All statutes which have modified and amended the Electronic Communications Act (also with Act. No. 247/2008 Coll, which transposed the Directive) may be found at:

   http://www.mpo.cz/dokument75810.html.

   List of Decrees and Government Regulations implementing the Electronic Communications Act, as subsequently amended may be found at: http://www.mpo.cz/zprava71491.html.

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

The Act. No. 247/2008 Coll. came into force on 5 June 2008 and came into effect on 1. 9. 2008. Therefore, there was a transition period of more than 2 months before its rules which modified the Electronic Communications Act were applied.

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

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

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

A legal area of data retention law is in the Czech legal system regulated mainly by the Electronic Communications Act and by the Decree No. 485/2005 Coll., on the extent of traffic and location data, the time of retention thereof and the form and method of the transmission thereof to bodies authorised to use such data (hereinafter only „Decree No. 485").

The Electronic Communications Act is the Act of Parliment which came into effect on on 1 May 2005. It determines the conditions of business activities and performance of state administration, including market regulation, in the electronic communications area on the basis of the law of the European Communities[1]. It modified the rules of the classic telecommunication services market, it applied also for a new kind of electronic communications services, e.g. cable television broadcasting or digital broadcasting. However, the Electronic Communications Act does not apply for the content of the services. The substantive obligation to retain

[1] Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).
Directive 2002/20/EC of the European Parliament and of the Council on the authorisation of electronic communications networks and services (Authorisation Directive).
Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services (Framework Directive).
Directive 2002/22/EC of the European Parliament and of the Council on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive). Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on Privacy and Electronic Communications).
Commission Directive 2002/77/EC on competition in the markets for electronic communications networks and services.
Directive 1999/5/EC of the European Parliament and of the Council on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity.

and transmit the data in accordance with the Directive (including a limitation of time period of retention) is stipulated in the Art. 97 par. 3 of the Electronic Communications Act. Some other obligations are stated in the Art. 88 par. 1, Art. 89 par. 1 (technically oriented obligations), in the Art. 97 par. 10, par. 11 (keeping and providing of records), in the Art. 97 par. 8 (confidentiality) of the Electronic Communication Act.

Consequently, Art. 97 par. 4 of the Electronic Communications Act states that the scope of traffic and location data retained, the period for the retention thereof and the form and method of their transmission to authorities authorized to use them, and the period for the retention and disposal of data provided to authorities authorized to request them under special legislation, shall be laid down in implementing legislation. In this case, such an implementing legislation is the Decree No. 485/2005 Coll. (hereinafter only „the Decree"). It must be noted, that legislation on data retention had existed in the Czech Republic before the Directive came into force (as mentioned in the point 1). Therefore, there was no need to update the Decree when the effective Directive was being transposed because the stipulations of Decree ware already in accordance with the Directive. Therefore, only the Electronic Communications Act was modified when transposing the Directive into the Czech legal system in 2008.

The Decree contains mainly the technical matters (technical definitions, technical description of the process of Extent of Traffic and Location Data Retention and Method of Data Transfer. It also contains a Time of Data Retention, but it must be taken into consideration, that limits of the time of data retention are determined directly by the Electronic Communication Act and the period mentioned in the Decree must comply with this limits.

It may be closed down, that more important matters and rules in the area of data retention in the electronic communications are engaged in the Act (Electronic Communications Act), which is a document approved by the Parliament and it has superior legal force than the Decree.[2]

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

The Czech national law defines only some terms used in Art. 2 par. 2 of the Directive. The definitions are contained in the Art. 2 of the Electronic Communications Act. Terms „user" and "unsuccessful call attempt" are definied in the same way as in the Directive. The terms „traffict data" and „localization data" are defined in the Art. 90 and 91 of the Electronic Communications Act and these

[2] In accorance with the Art. 95 of the Czech Constitution (Const. Act. No. 1/1993 Coll.): In making their decisions, judges are bound by statutes (acts) and treaties which form a part of the legal order; they are authorized to judge whether enactments other than statutes (acts) are in conformity with statutes (acts) or with such treaties.

definitions are strictly the same as mentioned in the directive 2002/58/EC. The other definitions mentioned in the Art. 2 of the Electronic Communicaton Act comply with the definitions of the Directives 95/46/EC, 2002/21/EC and 2002/58/EC.

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 Art. 97 par. 3 of the Electronic Communications Act traffic and location data which are generated or processed in the provision of its public communications networks and in the provision of its publicly available electronic communications services shall be retained. The traffic and location data relating to unsuccessful call attempts only shall be retained if these data are generated or processed and retained or recorded at the same time.

Further, the Decree specifies what kind of data must be retained and the obligation of subjects is specified more concretely than the extent of data mentioned in the Art. 5 of the Directive and it is also a little bit wider than the extent of data mentioned by the Directive. The Extent of Traffic and Location Data which shall be retained may be found in the Art. 2 of Decree. [3] For example, the operators are obliged to retain

[3] (1) The juristic or natural persons providing a public communication network or publicly accessible electronic communication service ("operator") shall submit the operation and location data defined herein ("data") to the body authorised to request such submission ("authorised body").
(2) For switched and fixed-connection electronic communication networks, the following data shall be maintained: a) data on the communication that has taken place, indicating the type of communication, the calling party's and called party's telephone number or identifier of the telephone card for use in the public pay phones, the communication start date and time, length of the communication and the status of the communication, where applicable; b) data on all the public pay phones, including their telephone numbers, registration numbers, geographical coordinates and verbal description of the location.
(3) For public electronic communications mobile telephone networks, the following data shall be maintained: a) data on the communication that has taken place, indicating the type of communication, the calling party's and called party's telephone number, the communication start date and time, length of the communication, the IMEI number, StartBTS station number and, where applicable, the StopBTS station, the destination, and additional information; b) data on the links between MSISDN numbers and IMEI numbers, jointly used in the network, identification of the BTS station and the IMEI number that made it possible to make a call without a SIM card to the emergency call number "112", the IP addresses of the terminals through which SMSs were sent via the Internet, the date and time of credit recharging for prepaid services, numbers of the recharging coupons in respect of a specific subscriber telephone number, and the subscriber telephone number in respect of a certain recharging coupon; c) data on all BTS stations with indication of their numbers, geographical coordinates, antenna azimuth and a verbal description of the location of the BTS station.
(4) For packet-switching electronic communication networks, the data on the communication that has taken place are maintained as follows: a) for the network access service – with indication of the type of connection, user account identifier, service user equipment identifier, connection start date and time, connection end date and time, identifiers related to the object of

the identifier of the telephone card for use in the public pay phones, data on all the public pay phones, including their telephone numbers, registration numbers, geographical coordinates and verbal description of the location in case of switched and fixed-connection electronic communication networks, in case of mobile telephone networks the IP addresses of the terminals through which SMSs were sent via the Internet, the date and time of credit recharging for prepaid services, numbers of the recharging coupons in respect of a specific subscriber telephone number, and the subscriber telephone number in respect of a certain recharging coupon. The operators are also obliged to retain data when the user is disposing with other electronic communication services as chat, usenet, instant messaging and IP telephones, in case of packet-switching electronic communication networks the operators have to retain quantity of transmitted data and information about the use of secured communication, the service request method and status.

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.

The retention of electronic communications data beyond the range of data to be retained in the terms of the Directive and the Electronic Communications Act is allowed in Art. 90 and 91 of the Electronic Communications Act. In compliance with these stipulations e.g. the traffic data essential for the billing of the price for the service provided may be retained until the end of the period within which the billing of the price can be legally challenged or the payment thereof collected or for the purposes of marketing the electronic communications services or for the provision of value-added services, the undertaking providing publicly available electronic communications service may retain the traffic data for the period as needed for such services or such marketing, as far as the subscriber or user to whom the data relate gave a consent thereto. However, the subscriber or user may withdraw his consent with the processing of traffic data at any time. Moreover, in case of location data the operator providing a public communications network or publicly available electronic communications service retains the data, such an operator shall render such data anonymous or gain the user's or subscriber's consent to the retaining of

---

interest (e.g. IP address, port number), event status (success, failure, normal/abnormal end of connection), quantity of transmitted data (incoming / outgoing); b) for the mailbox access services – with indication of the equipment identifier of the user who is the object of interest, the user account identifier, e-mail server message identifier, communication start date and time, sender's e-mail address, recipients' email addresses, e-mail protocol identifier, quantity of transmitted data and information about the use of secured communication; c) for the e-mail message transmission service – with indication of the equipment identifier of the user who is the object of interest, the e-mail server identifier, communication start date and time, sender's e-mail address, recipients' e-mail addresses, e-mail protocol identifier, quantity of transmitted data and information about the use of secure communication; d) for server services – with indication of the equipment identifier of the user who is the object of interest, the user account identifier, service request date and time, all server identifiers (including, but not limited to, the IP address, the fully qualified domain number FQDN), the required URI or service type dentifiers, additional parameters of the URI or service identifiers, the services used, the quantity of transmitted data, and the service request method and status; e) for other electronic communication services (including, but not limited to, those of the type of chat, usenet, instant messaging and IP telephony) – with indication of all the identifiers of the communicating parties, the transport protocol, communication start date and time, communication end date and time, the service used and quantity of the transmitted data.

such data to the extent and for the period as needed for the provision of value-added services. Before gaining the consent, the operator shall inform the concerned user or subscriber about the type of location data to be retained other than those of operating nature, about the purpose and length of the retention and whether the data are to be made available to a third party for the provision of value-added services. The user and subscriber may withdraw his consent with the processing at any time.

A retention of the content of communications is expressively forbidden in the Art. 97 par. 3 of the Electronic Communications Act.[4]

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

The purpose of the data retention in accordance with the Czech legislation is to keep possible to provide them immediately to authorities authorized pursuant to special legislation upon their request. Such an authority is defined for example in Art. 88a of the Act. No. 141/1961 Coll., on criminal proceeding (see more in point No. 14) or in the Act. No. 273/2008 Coll. on the Police of the Czech Republic. These authorities (mainly police) may consequently use the data for fulfillment of their targets and missions.

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)?

In accordance with the European directives[5] Czech legislatives approved Act No. 41/2009 Coll., on the Protection of Personal Data. This act regulates a retention and transmission of the sensitive data, which shall mean personal data revealing nationality, racial or ethnic origin, political attitudes, trade-union membership, religious and philosophical beliefs, conviction of a criminal act, health status and sexual life of the data subject and genetic data of the data subject; sensitive data shall also mean a biometric data permitting direct identification or authentication of the data subject.[6]

---

4 At the same time, this person (operator) shall ensure that the content of reports is not retained with the data referred to in sentences one and two. Yes, this is the direct wording.

5 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, amended by Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and also by Directive 2009/136/EC

6 Article 9 of Act No. 41/2009 Coll.
Sensitive data may be processed only:
(a) if the data subject has given his express consent to the processing. When giving his consent, the data subject must be provided with the information about what purpose of processing, what personal data, which controller and what period of time the consent is being given for. The

A special regulations applies in case of the Czech Police, which may operate with the personal data including sensitive without the consent of the person, if it is necessary for the fulfillment of its objectives, all in accordance with the Art. 79 of the Act. No. 273/2008 Coll., on the Police. Nevertheless, the Police is entitled to keep the data concerning racial or ethnic origin, political attitudes, sexual life and the membership in the organization, which is not prohibited by the law only with regard to the concrete individual criminal proceeding.

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

The Electronic Communications Act stipulates limits of the period for retaining traffic and location data, which is between 6 and 12 months. Consequently, the Decree specifies, that data shall be retained for 6 months, but in case of the server services the requested URI identifier or any other service identifier and URI or service identifier shall be stored only for 3 months. However, the 3 months period is from our point of view in contradiction with the limits mentioned by the Electronic Communications Act but it complies with the Directive, because the retention of this specific data goes beyond the Directive's stipulations.

---

controller must be able to prove the existence of the consent of data subject to personal data processing during the whole period of processing. The controller is obliged to instruct in advance the data subject of his rights pursuant to Articles 12 and 21,
(b) if it is necessary in order to preserve the life or health of the data subject or some other person or to eliminate imminent serious danger to their property, if his consent cannot be obtained, in particular, due to physical, mental or legal incapacity, or if the data subject is missing or for similar reasons. The controller shall be obliged to terminate data processing as soon as the above mentioned reasons cease to exist and must liquidate the data, unless the data subject gives his consent to further processing.
(c) if the processing in question is in relation with ensuring health care, public health protection, health insurance, and the exercise of public administration in the field of health sector pursuant to a special Act, or it is related to assessment of health in other cases provided by a special Act,
(d) if the processing is necessary to keep the obligations and rights of the controller responsible for processing in the fields of labour law and employment provided by a special Act,
(e) if the processing pursue political, philosophical, religious or trade-union aims and is carried out within the scope of legitimate activity of a civil association, foundation or other legal person of non-profit nature (hereinafter referred to as the "association"), and which relates only to members of the association or persons with whom the association is in recurrent contact related to legitimate activity of the association, and the personal data are not disclosed without the consent of data subject,
(f) if the data processed pursuant to a special Act are necessary to carry on sickness insurance, pension insurance (security), accident insurance, state social support and other state social security benefits, social services, social care, assistance in material need and social and legal protection of children, and if, at the same time, the protection of these data is ensured in accordance with the law,
(g) if the processing concerns personal data published by the data subject,
(h) if the processing is necessary to secure and exercise legal claims,
(ch) if they are processed exclusively for archival purposes pursuant to a special Act, or
(i) if it is the processing under special acts regulating prevention, investigation, detection of criminal activities, prosecution of criminal offences and search for persons.

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)?

The authorities which are entitled to access the data retained are specified directly nor in the Electronic Communication Act neither in the Decree. The authorization is given to the authorities by other legal statutes. Presently, the authorized body is mainly the Police, which may access to the retained data in accordance with the Act. No. 273/2008 Coll. on the Police of the Czech Republic. According to the Art. 71, the police may require the retained data in the case of prevention or disclosing of a danger in the field of terrorism. According to the the Art. 68 par. 2 of the Act, the Police may require the retained data when it is searching for some missing person or with the aim of discover an identity of some person or dead body. Finally, the Police may in accordance with the Art. 66 par. 3 of the Act. require the retained data in the cases mentioned by the law and in the range necessary for the fulfillment of some individual mission (objective).

The mentioned stipulations go together with the Art. 88a of the Act. No. 141/1961 Coll., on criminal proceeding, under which the entitled bodies which may access the data are a tribunal of judges, an individual judge and during the preliminary proceeding a public prosecutor or the Police, always under the condition that these data are usable for a clarification of important facts in the criminal procedure.

Other state authorities are not entitled to access the retained data directly by the Act. Nevertheless, the Art. 78 of the Act. No. 273/2008 Coll. on the Police of the Czech Republic stipulates very important rule of cooperation between the Police and information services (as Military Information Service and Security Information Service), military police, ministry, prison services, custom-duty authorities and other authorities of the public administration. Under this rule the police transmit to the mentioned authorities information (including information from the police evidence) which obtained during the fullfilment of its missions as far as it is necessary for the fullfilment of the missions (objects) of the mentioned authority.

The Police is not obliged to transmit the data if such a transmisson may endanger the fullfilment of the police missions (objects).

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)?

In the Electronic Communications Act and neither in the Decree is not exactly stipulated for which purposes retained data may be used (with exemption mentioned in par. 10). Presently, the data retained which is available to the bodies in the criminal proceeding with regard to the Art. 88a of the Act. No. 141/1961 Coll., on criminal proceeding as mentioned above may be used only in this procedure for a clarification of important facts in the criminal procedure, however, no legal act defines in what kind of criminal procedures the authorities may obtain the data from

operators. Therefore, the entitled authorities may ask for the retained data also in cases of crimes which are not very serious.

As it is mentioned in the point No. 14 of this report, the Police may require the data in accordance with the Act. No. 273/2008 Coll. on the Police of the Czech Republic for following purposes:

- prevention or disclosing of a danger in the field of terrorism (Art. 71);
- searching for a missing person or discovering the identity of somebody or a dead body (Art. 68 par. 2);
- for the fulfillment of some individual mission (objective) in the necessary range (Art. 66 par. 3).

On the other hand, no authority is entitled for access to the retained data in case of administrative offences. Also it is not possible for individuals to claim and to request the retained data in case by civil actions.

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)?

When some authorized body mentioned in the Art. 88a of the Act. No. 141/1961 Coll., on criminal proceeding intends to access to the retained data, the following conditions must be fulfilled:

- these data are usable for a clarification of important facts in the criminal procedure;
- order of a tribunal of judges and in the preliminary proceeding order of a judge has to be given in writing and with appropriate statement of the reasons.

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?

As mentioned in the par. 16 it is necessary to obtain the court (judge) order before accessing the retained data[7], nevertheless, the law does not require to hear the aggrieved party or to involve him/her otherwise in the proceeding. The court order shall contain what data may be accessed, for what period, the purpose for accessing the data, ets. The aggrieved party has no right of appeal and it is not notified about such an order.

[7] See also information of the Police official websites – http://www.policie.cz/clanek/provozni-a-lokalizacni-udaje-o-komunikaci.aspx

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?

The Czech legislation does not provide that the aggrieved party shall be notified of a data access.

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

The Czech legislation also does not stipulate exactly that the aggrieved party has a right to be informed about the data accessed in case these data are related to him/her.

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?

No, the aggrieved party has no direct recourse to the courts in case their data were transmitted to some of the authorized bodies.

However, in the Czech legal system exist some possibilities how to claim damages caused by the entitled authorities when accessing the data. The aggrieved party may use a civil action concerning a protection of personality or the civil action according to Act. No. 82/1998 Coll. on the liability for damage caused by the public authority or the wrong official procedure.

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.

As the legal provisions protecting the data retained against unauthorized access may be considered the stipulations of the Art. 3 of the Decree. In accordance with these rules the following shall be used to prove the authenticity of the request and the data being transferred:

- guaranteed electronic signature, based on a qualified certificate issued by an accredited certification service provider;
- cover letter in paper form, containing the reference number or serial number of the request, the file name, the date, time and method of hand-over and possibly also the checksum or standard hash of the file (e.g. SHA-1), and signature of an authorised person;
- letter in paper form, containing the reference number and signature of an authorised person;
- in the case of requests or data already transferred in an electronic format for a certain period, which as a rule is one week, for which no other authenticity proof

has been used: a letter in paper form, which is sent subsequently, containing the reference number and signature of an authorised person.

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

If the transmitted data is used in the criminal procedure as the official measure of a proof it forms a part of court's (criminal) files and it is not destroyed. If the obtained data is not used by the authority as a proof there is no legal obligation stating a limit in which the accessed data shall be destroyed. The Act. No. 273/2008 Coll. on the Police of the Czech only states an obligation of the Police to keep identification information about the police body and the policeman who had asked for the data and about the purpose of data accessing for the period of 5 years.

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.

Any legal or natural person providing a public communications network or providing a publicly available electronic communications service must retain traffic and location data which are generated or processed in the provision of its public communications networks and in the provision of its publicly available electronic communications services. The Electronic Communications Act does not distinguish any group of neighbouring services.

A database of the Czech Telecommunication Office contains more than 2000 subjects (legal or natural person in accordance with the definition above). All of these subjects are obliged to retain the data, however, in reality probably only the biggest providers comply with their obligations.

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 are no exemptions in the group of subjects which are obliged to retain traffic and location data as mentioned in the Art. 97 of the Electronic Communications Act.

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?

Due to the fact that the Electronic Communications Act took into account the Directive already in 2005, when the Directive was being prepared, since 2005 when it came into force it has already contained the very similar range of data categories that have to be retained nowadays, after the transposition of the Directive. The only

exemption in the data range, which was not covered by the original text of the Act before the Directive came into force are the data related to unsuccessful call attempts.

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)?

Following the other legal obligations on data security than those mentioned in point 21 of the report are mentioned.

The undertaking providing publicly available electronic communications service is obliged with regard to the Art. 88 of the Electronic Communication Act to:

- take technical and organizational measures to safeguard the security of the service in respect of the protection of the traffic and location data; if necessary, the provider concerned shall upon written agreement also co-operate with the undertaking providing the communications network to provide the protection,

- ensure that traffic and location data retained in accordance with the Art. 97 par. 3 are of the same quality and are subject to the same security and protection as traffic and location data in the provision of an electronic communications services,

- prepare internal technical and organizational regulations to provide data protection and communications confidentiality in accordance with Clause above; secure data protection and communications confidentiality with respect to the existing technical capabilities and the costs needed to provide protection at a level adequate to the risks of compromising the protection.

Only the person who legally undertakes a business (including all legal persons) must comply with these obligations, however, we suppose that no natural person who is not an undertaker may legally provide publicly available electronic communications service.

Moreover, a legal or natural person providing a public communications network or providing a publicly available electronic communications service and its employees shall respect the confidentiality of the request and provision of traffic and location data, including any circumstances relating thereto.

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)?

From our point of view, there are no substantive additional costs for the providers with regard to the transposition of the Directive in 2008 due to the fact that the Electronic Communications Act took into account the Directive already in 2005, when the Directive was being prepared. Moreover, the providers receive reimbursements from the Czech Republic (in concrete see next point No. 28). Some

additional costs might have originated to the Czech Telecommunication Office – costs joined with the administration of the subjects obliged to retain data and with the supervision of them.

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?

The legal entity or natural person is entitled to be reimbursed for the **efficiently** incurred costs for fulfillment of the obligations concerning the traffic and location data retention from the entitled authority that requested an access to the retained data. The amount and a method of reimbursement for the efficiently incurred costs is being specified by implementing legal regulations, in concrete the decree No. 486/2005 Coll. laying down the amount and method of reimbursement of effectively spent costs for the establishment and securing of an interface for connection of terminal telecommunication equipment for wiretapping and recording of messages and for storage and provision of operating and localization data and for provision of information from the subscriber database of a publicly available telephone service. According to the decree the amount of costs for the retention of traffic and localization data is determined as a sum of book depreciation items of the equipment serving for its storage and of costs spent for securing this equipment. The exact amount of costs for the provision of traffic and localization data is set out in Part I of Annex to the Decree.

For example, the spokesman of the company T-Mobile Czech Republic notified, that the amount of reimbursement during one year is in millions of Czech Crowns.

The entitled company has to proove that the costs were incurred efficiently.

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

The cooperation between the subject retaining the data and the authorized body which may request the access to the data is ruled by the Decree, especially Art. 3 of the Decree where the process and Method of Data Transfer is described[8].

[8] (1) An authorised body may, through its assigned contact workplace, ask the operator to make the stored information available. The operator shall immediately deliver the requested data through its assigned contact workplace. The data referred to in Section 2(3)(c) shall be handed over on a monthly basis in a summarised form up to date as at the handover date.
(2) Communication between the contact workplaces of the operator and the authorised body shall preferably be provided in a manner allowing for remote access. Requests and data shall preferably be delivered in a data file electronic format. Generally available technologies and communication protocols shall only be used in the contact workplaces' communication so as to avoid linking the solution to a specific manufacturer or supplier.
(3) Where it is impossible or unreasonable to use for communication a method allowing for remote access, an application or the requested data can be provided in paper form or in data files on a portable medium.
(4) The following shall be used to prove the authenticity of the request and the data being transferred:

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

The Electronic Communications Act regulates in the Art. 118 a regime of administrative offences of legal entities and undertakings who are natural persons.

A legal entity or a natural person who is an entrepreneur commits administrative offence if it does not comply with its obligation stated by the Art. 97 of the Act (see point 8 and 9). As a sanction a financial penalty may be imposed for the infringement of the provisions up to CZK 10,000,000 or up to 10% of the proceeds

---

a) guaranteed electronic signature, based on a qualified certificate issued by an accredited certification service provider1); cryptographic standard format with the PKCS#7 public key shall be used to create and validate the signature;
b) cover letter in paper form, containing the reference number or serial number of the request, the file name, the date, time and method of hand-over and possibly also the checksum or standard hash of the file (e.g. SHA-1), and signature of an authorised person;
c) letter in paper form, containing the reference number and signature of an authorised person; or
d) in the case of requests or data already transferred in an electronic format for a certain period, which as a rule is one week, for which no other authenticity proof has been used: a letter in paper form, which is sent subsequently, containing the reference number and signature of an authorised person.
(5) Data on the communication that took place under a certain identifier for a certain period of time shall be handed over by the operator to the authorised body as:
a) fixed line communication dump, for data referred to in Section 2(2)(a) - data on the communication that has taken place, indicating the type of communication, the calling party's and called party's telephone number or identifier of the telephone card for use in the public pay phones, the communication start date and time, length of
the communication and the status of the communication, where applicable;
b) mobile communication dump, for data referred to in Section 2(3a) - data on the communication that has taken place, indicating the type of communication, the calling party's and called party's telephone number, the communication start date and time, length of the communication, the IMEI number, StartBTS station number and, where applicable, the StopBTS station, the destination, and additional information;
c) data communication dump, for data referred to in Section 2(4).
(6) The communication dumps referred to in Section 5 above shall be handed over to the authorised body in a structured text file, preferably with coding based on the CP-1250, UTF-8 or ISO 8859-2 character set. The files are prepared separately for each single telephone number or any other identifier indicated in the request. The names of the files being transferred are structured on the basis of the name convention given in the Annex.
(7) The files have a uniform heading and a fixed structure, determined for the given type of network, or service, or request. The individual lines in the file are arranged chronologically, unless any other arrangement parameter is indicated in the request. The dump referred to in Subsection 5 above ends with the word "Konec" (End) in the last line.
(8) Within the line, the individual data elements are separated by the semicolon (code 0059 of the character set) or tabulator (code 0009 of the character set). The last item terminates with the CRLF character (codes 0013 and 0010 of the character set). If any of the data elements is not required or can be proved not to be identifiable with the technology used, its place in the structure shall be left empty.
(9) For information consisting of more than one data value, the individual values shall be separated by the "|" character (code 0166 of the character set). In the case that a character contained in the information being transferred is the same as any of the above separators, or if there is the character "\"(code 0092 of the character set), it must be prefixed with "\" (for example: "\;", "\CR\LF", "\\").
(10) In justified cases and with the consent of an authorised body and the operator, it is possible to use a file format, structure and name different from the specification in Subsections 6 to 9.

of the person on whom the fine is imposed as reported for the last completed financial year, up to a maximum of CZK 10,000,000. A legal entity or an undertaking who is a natural person shall not be responsible for an administrative offence if he/it is able to prove having exerted all efforts as could be required to prevent breaching the legal obligation. Responsibility of the legal entity or the undertaking who is a natural person for administrative offences shall lapse if the administrative body did not initiate any proceedings relating thereto within 3 years of learning about such an administrative offence and, at the latest, within 10 years of such offence's being committed. In determining the amount of the fine to be imposed on a legal entity or an undertaking who is a natural person, account shall be taken of the seriousness of the offence including, but not limited to, the manner in which it was committed, its consequences, its duration, and the circumstances in which it was committed.

The Act. No. 40/2009 Coll., Criminal Code contains only the crime – Infringement of a secret of messages being delivered (Art. 182). However, this crime cannot be applied for the infringement of data retention obligation, because it may be applicable only when somebody breaches the rules on the protection of the content of the message.

Dimension 3 (State – State)

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

There is no public body responsible for establishing the contact between the entitled body and the party retaining the data. The cooperation is direct between the public authority (mainly police) and private person retaining the data.

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 are no regional entities that have been granted their own rights of access to the retained data.

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?

The Decree (mainly the Art. 3) governs a co-operation between the entitled authorities and the subjects retaining data (see point 29 of the report). No other rules have been approved for governing e.g. the exchange of the retained data between the entitled bodies in different matters etc.

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)?

In accordance with the Art. 80 par. 6 of the Act. No. 273/2008 Coll. on the Police of the Czech Republic the Police is entitled to transmit the personal data to the foreign country in following cases:

- when using the Schengen informative system;
- or with regard to different aims of criminal procedure to a) Interpol; b) European Police Authority; c) foreign safety authority; d) respective authority or institution of the EU member state.

However, these authorities may require data only in cooperation with the Police of the Czech Republic, they may not access the retained data directly from the providers obliged to retain it.

Moreover, Council framework Decision 2008/977on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters may not be taken into account, because the Czech republic has not taken the necessary measures to comply with the provisions yet.

Also the Convention on Cybercrime does not apply, because the treaty has not been ratified yet (signature of the Czech republic is dated 9 February 2005.

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 Czech Telecommunications Office (hereinafter referred to as "the Office") is a central administration body (it is independent without a ministry as a superior authority) with responsibility for state administration in matters set out in Electronic Communication Act.

The Office is an accounting entity and it has a separate chapter in the State Budget of the Czech Republic. The Office is entintled to control both, legality and technical advisibility, if such is stated by the Electronic Communication Act or the related legislation.

Moreover, the Office for the Personal Data Protection as independent authority is the authorized body for monitoring compliance with the obligations in processing personal data according to Electronic Communications Act, e.g. a time of data retention (Art. 87 par. 3).

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?

If so, please answer to the following questions:

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

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

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

In March 2010 a constitutional lawsuit (ústavní stížnost) was signed and filed by fourty six deputies. A text of the lawsuit was prepared by the non-governmental organization Iuridicum Remedium and the signatures of deputies facilited to comply with conditions of the Act No. 182/1993 Coll, on the Constitutional court, because the Act requires at least 41 deputies for such a lawsuit.

The Art. 97 par. 3 and 4 of the Electronic Communication Act and also the Decree are alleged to be contrary the Constitution of the Czech Republic in the lawsuit. Ruling has been issued yet in this proceeding.

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

We are not aware of any lawsuit with European courts filed by some Czech subject.

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

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

Legal rule governs where the retained data has to be stored by the obliged person. We suppose that the majority of the providers store the data at their own premises, however, we cannot except, that some of them (mostly smaller providers of services) may store data using external specialized subjects.

39. Are data stored outside the country or would this be permissible according to national law? If either of these cases applies: what data protection rules have the companies involved in the storage (both in your country and abroad) been obligated to?

The Czech law does not regulate data retention outside the country. The subjects involved in the storage of data are obliged to comply with the Art. 89 of the Electronic Communications Act, which stipulates that the undertakings providing public communications networks or publicly available electronic communications services shall ensure the technical and organisational measures to safeguard the confidentiality of the messages and the traffic and location data, which are transmitted via their public communications network and the publicly available electronic communications services. In particular, such undertakings shall not admit any tapping, message storage, or any other types of interception or monitoring of messages, including the data contained therein and related thereto, by any persons other than the users, without the consent of the users concerned, unless otherwise provided in laws.9 This shall not be to the prejudice of the technical storage of data as needed for message transmission without affecting the confidentiality principle.

Moreover, the obligatins mentioned in the Art. 88 par. 1 of the Electronic Communications Act should be taken into account (see point 26 of this report).

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

a) no data are retained beyond what is permitted?

No technical or organizational measures ensure in practice that no data are retained beyond what is permitted. However, The Czech Telecommunications Office and Office for the Personal Data Protection (in case of the personal data) may impose a penalty in case the subject fails to comply with the duty specified in Art. 97 par. 3 and par. 4 of the Electronic Communications Act, which stipulates a period for data retention.

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 case the subjects retaining the data did not observe the rules and would give the data to the state bodies without the respective court order, it might be possible to impose the penalty for administrative offence in the same way as mentiond in the paragraph above.

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

We are not aware of any measures which would be usable to avoid a misuse of data for other purposes.

---

9 It means especially Art. 97 par. 3 of the Electronic Communicatons Act.

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

The bodies accesing to the retained data (tribunal of judges, an individual judge and during the preliminary proceeding a public prosecutor or mainly the Police) store the data in the respective files, which are kept in accordance with the Act. No. 499/2004 Coll., on archival science and files services.

The subjects retaining the data have to prepare internal technical and organizational regulations to provide data protections in accordance with the Art. 88 Par. 1 letter b) on the Electronic Communications Act.

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

There is no direct legal obligation to destroy the retained data, however, it seems to be logical to destroy them after the 6 month period for retention expires. The Czech law does not stipulate anything about a safeness of the data destructure.

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)?

The aggrieved party is not notified.

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

When retaining the sensitive data, the subjects shall be registered at the Office for the Personal Data Protection which is entitled to control the fulfillment of the obligations stipulated in Act No. 41/2009 Coll. on the Protection of Personal Data.[10]

---

[10] Article 9 / Sensitive Data
Sensitive data may be processed only:
(a) if the data subject has given his express consent to the processing. When giving his consent, the data subject must be provided with the information about what purpose of processing, what personal data, which controller and what period of time the consent is being given for. The controller must be able to prove the existence of the consent of data subject to personal data processing during the whole period of processing. The controller is obliged to instruct in advance the data subject of his rights pursuant to Articles 12 and 21,
(b) if it is necessary in order to preserve the life or health of the data subject or some other person or to eliminate imminent serious danger to their property, if his consent cannot be obtained, in particular, due to physical, mental or legal incapacity, or if the data subject is missing or for similar reasons. The controller shall be obliged to terminate data processing as soon as the above mentioned reasons cease to exist and must liquidate the data, unless the data subject gives his consent to further processing.

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)?

Bigger companies often hire external auditors with the aim to revise if they comply with the obligations stipulated by the Electronic Communications Act. The control of the authorized state bodies should be realized by The Czech Telecommunications Office and the Office for the Personal Data Protection. Nevertheless, from our point of view the control is realized mainly in big companies, which are obliged to retain data (as T-Mobile, Telefonica, Vodafone, UPS).

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?

Some technical standards of the concerning the transmission of the data in dumps de iure are mentioned in the Art. 3 par. 6, 7, 8 and 9 of the Decree.[11] In practice the

---

(c) if the processing in question is in relation with ensuring health care, public health protection, health insurance, and the exercise of public administration in the field of health sector pursuant to a special Act, or it is related to assessment of health in other cases provided by a special Act,
(d) if the processing is necessary to keep the obligations and rights of the controller responsible for processing in the fields of labour law and employment provided by a special Act,
(e) if the processing pursue political, philosophical, religious or trade-union aims and is carried out within the scope of legitimate activity of a civil association, foundation or other legal person of nonprofit nature (hereinafter referred to as the "association"), and which relates only to members of the association or persons with whom the association is in recurrent contact related to legitimate activity of the association, and the personal data are not disclosed without the consent of data subject,
(f) if the data processed pursuant to a special Act are necessary to carry on sickness insurance, pension insurance (security), accident insurance, state social support and other state social security benefits, social services, social care, assistance in material need and social and legal protection of children, and if, at the same time, the protection of these data is ensured in accordance with the law,
(g) if the processing concerns personal data published by the data subject,
(h) if the processing is necessary to secure and exercise legal claims,
(ch) if they are processed exclusively for archival purposes pursuant to a special Act, or
(i) if it is the processing under special acts regulating prevention, investigation, detection of criminal activities, prosecution of criminal offences and search for persons.

[11] (6) The communication dumps referred to in Section 5 above shall be handed over to the authorised body in a structured text file, preferably with coding based on the CP-1250, UTF-8 or ISO 8859-2 character set. The files are prepared separately for each single telephone number or any other identifier indicated in the request. The names of the files being transferred are structured on the basis of the name convention given in the Annex.
(7) The files have a uniform heading and a fixed structure, determined for the given type of network, or service, or request. The individual lines in the file are arranged chronologically, unless any other arrangement parameter is indicated in the request. The dump referred to in Subsection 5 above ends with the word “Konec” (End) in the last line.
(8) Within the line, the individual data elements are separated by the semicolon (code 0059 of the character set) or tabulator (code 0009 of the character set). The last item terminates with the CRLF character (codes 0013 and 0010 of the character set). If any of the data elements is not required or can be proved not to be identifiable with the technology used, its place in the structure shall be left empty.
(9) For information consisting of more than one data value, the individual values shall be separated by the “|” character (code 0166 of the character set). In the case that a character contained in the information being transferred is the same as any of the above separators, or if

majority of the operators retaining the data comply with these conditions. On the other hand, no legal rules concerning the technical standards of retention and interoperability between the operators and accessing authorities were approved in the Czech legal system.

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.

The cooperation between the authorized body and the operatro retaining the data is effected in accordance with the respective stipulation of the Decree. The authorised body through its assigned asks the operator to make the retained information available. The operator shall immediately deliver the requested data through its assigned contact workplace. Requests and data shall preferably be delivered in a data file electronic format. However, a classic (paper) form is also used often (more see in point 29).

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?

Based on our knowledge, there is no common working language for the cross – border requieres. The applications are mostly translated to the national language of the respective state. The procedure concerning the requests to the foreign countries is governed by the Act. 141/1961 Coll., On criminal proceedings.

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).

Basically, the knowledge of the Czech society about data retention problematic is not very wide. The majority of citizens are not informed in detail.

Some serious discussions concerning the data retention in the societey begun when the rules of the providers' reimbursement were being approved. From the economic point of view the companies which are obliged to retain data enjoy now the benefit of being paid for the data retention and for the accessing the data by the state authorities. The present system is quite beneficiary for the operators due to a fact

---

there is the character "\"(code 0092 of the character set), it must be prefixed with "\" (for example: "\;", "\CR\LF", "\\").

that a subject which remunerates them for such a service is the Czech Republic through its public bodies (as e.g. Police).

Quite high pressure for approvement of the Electronic Communications Act and the consequent act transposing the Directive was realized from a minester of industry and trade, Martin Říman (ODS - The Civic Democratic Party[12]). It might be possible that this pressure had its origine in the companies retaining the data which were interested in the data retention from the economic point of view.

In November 2007 Mr. Říman also suggested an approval of the Electronic Communications Act's modification, under which the Security Information Service and Military Information Service would be other entitled body to access the data. However, he stopped with its activity after the reaction of media and some deputies.

Unfortunately, the Security Information Service and Military Information Service actually can access to the retained data through the Police of the Czech Republic in accordance with the Art. 78 of the Act. No. 273/2008 Coll. on the Police of the Czech Republic (the Act was approved one year later – more point 14 of the report) and nobody in society mentioned this circumstance.

Actually, a new bill stipulating an authorization of mentioned agencies to the direct access to retained data was moved to the deputies.

Civil righs groups, as for example Iuridicum Remedium, were against the stipulations of the Electronic Communications Act and also against a transposition of the Directive into the Act as it was realized, due to the fact that , the stipulations which would protect basic human rights are missing in the transposition. Consequently, this organization has prepared the text constitutional lawsuit, which was signed by the deputies and filed to the Constitutional Court.

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 some other important obligations to retain data in the Czech Republic, mainly the following.

Personal data of employees – the employer is obliged to retain data of its employees for the purpose of keeping the salary agenda and for the purpose of fullfilment of the obligatins stipulated in the labour, tax and social-security law.

According to the Act. No. 273/2008 Coll. on the Police of the Czech Republic the Police is entitled to access the information about the time and place of usage of the electronic payment measure. Banks are obliged to retain such a data and the Police is entitled to access the bank system on-line.

12 The Civic Democratic Party, abbreviated to ODS, is the largest centre-right political party in the Czech Republic. It holds 53 seats in the Chamber of Deputies, making it the second-largest party.
The ODS is liberal conservative, and is notably Eurosceptic.

Visa Waiver – a complex of the international contracts with regard to the non-visa traveling of the Czech citizens to USA. The USA authorities are entitled to access to the Czech databases with citizens personal data including biometrical data.

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

The Czech Telecommunications Office shall prepare the statistics in accordance with the Electronic Communications Act for the Commision of EU. A legal or natural person providing a public communications network or providing a publicly available electronic communications service shall keep records

- of the number of cases in which, on request, it has provided traffic and location data to authorities authorized to request such data,

- of the period which has passed in individual cases where it has initiated the retention of traffic and location data up to the date on which an authorized authority requests such data, and

- the number of cases where it was unable to comply with a request for traffic and location data."

A legal or natural person providing a public communications network or providing an electronic communications service shall submit to the Office these records, in summary, for the previous calendar year in electronic form. The records submitted shall not contain personal and identification data. The Office shall forthwith forward a summary of the records received to the Commission."

However, the statistics are not publicly available on any website of the Czech Telecommunications Office.

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

We are not aware of such 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?

The main discussion in the Czech republic is actually about the constitutional lawsuit and about a new bill which would stipulate that also the Security Information Service (BIS) is entitled body to access the data.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law[13] **– considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?**

The fundamental rights protecting privacy, personal data and the secrecy of telecommunciations are determined by the constitutional act – Charter of fundamental rights and basic freedoms a part of the constitutional order of the Czech Republic. The basic fundamental rights that may be breached by data retention are stipulated in Art. 7 protecting the inviolability of the private life of the person[14], in Art. 10 par. 2 and 3 protecting private and family life and protecting the personal data[15] and in Art. 13 protecting the confidentiality of letters and records and communications sent by telephone, telegraph, or by other similar devices.[16] From our point of view, the actual regulation of data retention might breach also Art. 15 par. 1 protecting the freedom of thought, conscience, and religious conviction[17] and also some political rights mentioned in Art. 17 par. 1 and 2 protecting the freedom of expression and the right to information.[18]

Nor the Charter neither other constitutional law does specify which data may be considered as telecommunications content.

---

13 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).

14 The inviolability of the person and of her private life is guaranteed. They may be limited only in cases provided for by law.

15 Everyone has the right to be protected from any unauthorized intrusion into her private and family life. Everyone has the right to be protected from the unauthorized gathering, public revelation, or other misuse of his personal data.

16 No one may violate the confidentiality of letters or other papers or records, whether privately kept or sent by post or by some other means, except in the cases and in the manner designated by law. The confidentiality of communications sent by telephone, telegraph, or by other similar devices is guaranteed in the same way.

17 The freedom of thought, conscience, and religious conviction is guaranteed. Everyone has the right to change her religion or faith or to be non-denominational.

18 The freedom of expression and the right to information are guaranteed. Everyone has the right to express his views in speech, in writing, in the press, in pictures, or in any other form, as well as freely to seek, receive, and disseminate ideas and information irrespective of the frontiers of the state.

In accordance with Art. 10 [par. 3] of the Charter, everybody has the right to be protected from the unauthorized gathering, public revelation, or other misuse of his personal data, however, this constitutional rule does not prohibit to retain the data without a specific reason.

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

In accordance with the Art. 4 of the Charter it is possible to limit the exercise of the fundamental rights mentioned above under these conditions:

- Limitations may be placed upon the fundamental rights and basic freedoms only by law and under the conditions prescribed in the Charter.
- Any statutory limitation upon the fundamental rights and basic freedoms must apply in the same way to all cases which meet the specified conditions.
- In employing the provisions concerning limitations upon the fundamental rights and basic freedoms, the essence and significance of these rights and freedoms must be preserved. Such limitations are not to be misused for purposes other than those for which they were laid down.

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?

The national jurisprudence has not ruled on the constitutionality of the acts transposing the Directive yet.

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?

From the resolutions of the Constitutional Court has already arised that a balance of interests shall be carried in each individual case of fundamental rights 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)

No national constitutional rule does require directly that exemptions should be done in case of the obligation to retain the data.

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?

In our opinion the obligation of the subjects (operators) to retain the data does not breach their economic constitutional rights. The limits for such restrictions are mentioned in Art. 26 of the Charter, which stipulates: „Everybody has the right to the free choice of his profession and to the training for that profession, as well as to engage in commercial and economic activity. Conditions and limitations may be set by law upon the right to engage in certain professions or activities."

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)?

The national law does not allow any participation of the private subjects for the purpose of the law enforcement.

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

It is not imperative to reimburse the parties that are obliged to retain data in accordance with the Czech national constitutional law.

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?

The status of international treaties in the Czech legal system is set up in Art. 10 of the Constitution which stipulates: „promulgated treaties, to the ratification of which Parliament has given its consent and by which the Czech Republic is bound, form a part of the legal order; if a treaty provides something other than that which a statute (act) provides, the treaty shall apply."

Therefore, the promulgated treaties including the European Convention on Human rights are superior than regular statutes (acts) in hierarchy of Czech legal acts, however, they are not superior to the acts of the Czech constitutional order. This point is being often discussed by the Czech legal specialists and it might be one of the rules which will be modified in the Constitution in the future.

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?

For a transposition of directives a respecive legal enactment must be approved, mostly, it is a statute/act, however, it might be also the enactments of the lower legal power, e.g. regulations or decrees. There are no configurations that might concede to directives a particular statutes within the hierarchy of norms in the Czech republic

but it may be possible (although such a procedure is not used very often) to incorporate a text of the directive without any modifications into the legal body of a statute/act and approve it (adaptation).

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?

The possibility of transfering Czech national sovereignties to to the European Union was integrated to the Czech Constitution by the Art. 10a, which stipulates: „certain powers of Czech Republic authorities may be transferred by treaty to an international organization or institution. The ratification of a treaty under paragraph 1 requires the consent of Parliament, unless a constitutional act provides that such ratification requires the approval obtained in a referendum.“ Therefore, the limitation is given by the necesity of the approval of the respective treaty in qualified form.

A situation, when the competence already transferred to the European Union is exercised in conflict with the Czech national law is not regulated by any legal enactment and from our point of view it would depend on the interpretation of the Art. 10a of the Constitution in conjunction with a rest of the Constitution by the Czech Constitutional Court.

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

The Czech Telecommunications Office is the authority in the Czech Republic which has been given a major part of the powers with regard to the data retention (administration and supervision). The Office for the Personal Data Protection is a body authorized only for monitoring compliance with the rules of processing personal data.

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

The Czech constitutional law does not set any limit regarding the transmission of retained data abroad, however, a legal regulation approving such a transmission has to comply with the Art. 10 par. 3 of the Charter, which stipulates that „everyone has the right to be protected from the unauthorized gathering, public revelation, or other misuse of his personal data.“

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?

From our point of view the next basic points should be improved with regard to data retention rules and their possible breach into the basic human rights.

Traffic and localization data are being collected about everybody without any suspicion that a crime has been committed. Due to this fact the interference and breach into the constitutional right for privacy is not seemed as proporcional with the purposes of the data retention.

The law regulating rules of disposal of accessed data by the authorized bodies are not defined exactly, moreover through the Police the other state authorities may access the retained data. There is no legal regulation which would ensure the basic rights of a person when his/her data are being accessed (e.g. defence if the data are not correct or data are misused), even, the person is not notified about the data accession by the authorized bodies.

The Police may access the data when it is necessary for the fullfilment of its missions (objects), from our point of view the rules should state the exact range of crimes (mostly serious ones) when the accessment to data is allowed.

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

Czech Republic

Jan Fučík

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*?

The Charter of fundamental Rights and Freedoms is part of the Czech Constitution. It contains some provisions concerning privacy.

Art 13

No one may violate the confidentiality of correspondence or other secret documents and records whether privately kept or sent by mail or otherwise, except in cases and manner provided by law. It is to ensure confidentiality of messages by telephone, telegraph or other similar devices.

Art 10 §. 3

Everyone has the right to protection against unauthorized gathering, publication or other misuse of his personal data.

There is no explicit term „anonymously".

2. **Please illustrate in detail any amendments to current data retention legislation (which in the Czech Republic will after Consitutional Court's ruling supposedly be limited to access rules for entitled bodies) 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 § 2), discussed as a potential alternative to data retention?

The government of the Czech Republic approved in February 2012 proposal for an amendment of same laws. The proposal responds to the Constitutional Court judgment Pl. U.S. 42/11 of 20 December 2011, which repeals the provisions of § 88a of the Penal Code. For this reason the date of entry into force of the law was set at 1 October 2012.

The proposed amendment is divided into five parts, the first part amends the Electronic Communications Act so that it tightens the technical and organizational measures to protect traffic and location data, including their inspection, operators imposes the obligation to keep the stored provide data to competent authorities. The second part amends § 88a of the Penal Code so that set more stringent conditions for obtaining a permit to detect traffic and location data. The third part amends the Act on the Security Intelligence Service and the fifth part amends the Law on Military Intelligence so that it complements and clarifies the authority of the Security Intelligence Service and Military Intelligence. The law requires, that traffic and location data should be collected under conditions identical to wiretapping, i.e. permission of the presiding judge of the Supreme Court. The fourth part amends the Act on the Supervision of the capital market so that it specifies the purpose for which the Czech National Bank in exercising supervision over the capital market may request traffic and location data and the need to complement the prior written consent (permission) of the presiding judge of the High Court in Prague to demand data.

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?**

   Law Nr. 273/2008 Coll. on the Police Art.18

   Requiring assistance from individuals and institutions

   The policeman is the extent necessary to meet the specific task of the police power to require the institutions and persons referred to in § 14 (all) of the material and personal assistance, in particular the necessary documents and information including personal data. These bodies and persons are obliged to provide the assistance requested; do not do so, if prevented from doing so by legal or a public obligation of confidentiality or other legal obligations. A natural person may also do so if the provision of assistance has issued a serious threat to themselves or a close person.

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying**

commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?

The national law contains provisions concerning the rights of persons to refuse to testify/to deliver evidence against them selves. These rules do not include data to be retained and transmitted.

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

   The contested provisions of § 97 paragraph 3, third sentence of the Electronic Communications Act contains only a vague obligation for legal or natural persons in the range of traffic and location data retention, "on request, promptly provide the bodies authorized to request them under the special legislation." Although contested decree specifies in § 3, how are the individual cases to fulfill this obligation to the legitimate authorities, i.e., a relatively great detail defines a data transmission method of communication (electronic) format, used programs, codes, etc., but from the very amended under the provisions of § 97 paragraph 3 of the Act on Electronic Communications, nor the explanatory report by the Constitutional Court do not clearly show what kind of legitimate authorities, and what specific legislation specifically concerned. With regard to the wording of § 97 paragraph 1 of the Law on Electronic Communications, which establishes the obligation of legal or natural persons providing public communications network or providing publicly available electronic communications service, at the expense of the applicant to establish and secure the points for its network interface for connecting telecommunications terminal equipment for interception and recording of messages; one can only assume that even if the obligation to transmit the retention of traffic and location data are the same and similar institutions authorized by specific legislation, which addressed the enforcement authorities in criminal proceedings, apparently under § 88a of the Penal Code, Information Security service under § 6 and 8 of Act No. 154/1994 Coll. Security Intelligence Service, as amended, and Military Intelligence pursuant to § 9 and 10 of Law No. 289/2005 Coll. Military Intelligence. Thus defined rules allowing a massive interference with fundamental rights does not meet the requirements of certainty and clarity in terms of rule of law (see paragraph 37).

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.**

   According to a report on the security situation in the Republic for the year 2008 was in the Czech Republic found a total of 343.799 crimes, of which 127.906 were cleared of criminal acts while in the same period the number of requests for traffic and location data from authorized by public authorities, reached number 131.560

(cf. the EU Commission's report - "The Evaluation of Directive 2006/24/EC and National Measures to Combat the Criminal Misuse and Anonymous Use of Electronic Data, which have official information from the Czech asked, representatives of the Czech Republic's response to the questionnaire of 30 ninth 2009 are available on http://www.dataretention2010.net/docs.jsp). Consequently, not only for the period January to October 2009, according to unofficial data, the request for location and traffic data have already been made in 121.839 cases (cf. to Herczeg, J. constitutional limits monitoring of telecommunications: the conflict between security and freedom , Advocacy Bulletin No. 5 / 2010, p. 29).

B. Country-specific questions

7. Please describe the Constitutional Court's decision of 31 March 2011 in the case no. 24/10 on data retention (essential reasons of the ruling, legal consequence). Please also provide answers to the following questions:

Constitutional Court agreed with IuRe privacy protection activists and a group of 51 MPs who in March 2010 submitted a proposal calling for repeal of relevant sections of the Electronic Communications Act and implementing legislation imposing obligation on mobile operators and internet providers to retain data on communication for police use. The Court overturned certain provisions of the Electronic Communications Act. The Court found unconstitutional paragraphs 3 and 4 of section 97 of the Act, which had stipulated that telecommunications companies had to maintain records of customer Internet and telephone usage (including phone calls, faxes, text messages, Internet activity, and emails) for up to 12 months. The Electronic Communications Act Nr.127/2005 Coll. (in force on May 1, 2005) is based on the EU Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of public electronic communications services or public communications networks, which requires the EU Member States to gather telecommunications data in an effort to combat serious crime, in particular terrorism and organized crime. The judicial challenge to the Act was not in connection with the actual content of retained data but rather the information showing when and with whom people were communicating. According to the Court, ambiguously defined data retention rules result in measures applied for requesting and using retained data "being overused by authorities engaged in criminal proceedings for purposes related to investigation of common, i.e. less serious crimes". The Constitutional Courts also regards e.g. certain provisions of the Criminal Act concerning the use of such data by authorities engaged in criminal proceeding as highly questionable and it called on MPs to consider its modification. According to the Court, it will be necessary to consider each individual case in which data have already been requested in order to be used in criminal proceedings one by one – with respect to the principle of proportionality regarding privacy rights infringement. The decision implies that electronic communication providers are no longer obliged by any law to retain such data for the use of entitled authorities – as was previously the case according to the repealed provisions; the respective databases should be deleted.

8. **Does the ruling seek to strike a balance of the interests protected by fundamental rights and, where applicable, other norms enshrined in the constitution or having constitutional status? If so: which elements/aspects did the court consider when trying to strike this balance, and what was the result of such assessment? Please explain the impact of the proportionality rule in this context.**

   The Czech Constitutional Courts has consistently held, particularly in relation to the issue of interception of telephone calls, makes clear that the protection of the right to respect for private life in the form of a right to informational self-determination within the meaning of Article 10, paragraph 3 and Article 13 of the Charter of Rights applies not only to their own content of messages by telephone, but also information on numbers dialed, the date and time of call, its duration, for mobile telephony base stations for the call [cf. such as finding sp. No. II. CC 502/2000 of 22 1st 2001 (N 11/21 SbNU 83) - "the privacy of every person is worthy of the fundamental (constitutional) protection not only in relation to the equity content of their reporting, but also in relation to those mentioned above. It can thus be concluded that Article 13 of the Charter establishes the protection of secrecy dialed numbers and other related information such as date and time of call, its duration, if calling a mobile phone and base stations for signs call. (...) These data are an integral part of communication made by telephone. "- or similar findings No. IV. U.S. 78/01 of 27 8th 2001 (N 123/23 SbNU 197), sp. U.S. No. I. 191/05 of 13 9th 2006 (N 161/42 SbNU 327) or SP. No. II. CC 789/06 of 27 9th 2007 (N 150/46 SbNU 489)].

9. **What will happen to data that had been retained before the ruling? Is there an obligation to destroy these data?**

   There is no special obligation contained in the Constitutional Courts decision to destroy these data. They will be deleted in due time.

10. **What will happen to data retained that had been requested by any of the entitled bodies (police etc)? May they be used by these bodies/in a court proceeding?**

    Applicability of requested data for the purposes of criminal proceedings will be considered by the ordinary courts in terms of proportionality of interference with the right to privacy in each individual case. Courts will have to weigh the particular seriousness of the offense, which should be filled with a crime for which defendants in criminal proceedings in which the required data to be used.

11. **Please provide an overview of reactions of political and social groups to the ruling of the Constitutional Court (see question 7). Is it envisaged to table new legislation in order to bring national law in line with the Directive?**

    Most of reactions of political and social groups to the ruling of the Constitutional Courts were positive. The police told the investigation of crimes will be more difficult.

It is envisaged to prepare new legislation in order to bring national law in line with the Directive.

The following questions on peculiarities of the national transposition of the Directive refer to the legal situation in force before the Constitutional Court's decision (see question 7):

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

The court order for interception and recording of telecommunications traffic may be issued only in duly instituted criminal proceedings for legally qualified criminal activity, and must be supported by relevant some indication of which can be inferred reasonably suspected of committing such crime. The order must be individualized to a specific person who is a user's telephone station. Finally, it must command at least a minimum level to specify which facts relevant to criminal proceedings shall be determined as follows from what is inferred.

13. 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 (see your answer to question 9)?

Contested provisions of § 97 paragraph 3 and 4, became part of Act No. 127/2005 Coll. under Act No. 247/2008 Coll., amending Act No. 127/2005 Coll., on electronic communications and amending some related Acts (Electronic Communications Act), as amended. According to the explanatory report, the adoption of this amendment was used to implement "certain elements" of the European Parliament and Council 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC which are not yet in our legal system implemented, or are only partially implemented. Existing legislation in some respects is broader than that contained in the directive on data retention. The issue of retention of traffic and location data is in the Czech legal order in a modified form adapted from the actual adoption of the Electronic Communications Act No. 127/2005 Coll. with effect from 1. 5. 2005. The extent of traffic and location data, retention time and the form and manner of transfer of bodies authorized to use them is adopted with effect from 15. 12. 2005. At that time the EU had only prepared the data retention directive, which was actually in the Czech Republic effectively implemented in advance and the actual wording of the contested provision is required by the Directive on data retention. It is only a clarification of the obligation to retain traffic and location data and provide this information promptly to the authorized bodies their request. The contested ordinance despite this fact, however, have not been altered, resulting in the fact that the contested legislation regulated the extent of the stored data remain

clearly above the anticipated within the scope of the Directive is about data retention.

The obligations of telecom operators, Internet service providers and others who work in the field of electronic communications to store for at least 6 months location and traffic data was presented this way: "in any case this is not something that could be like wiretapping. There is no stored content of calls or email messages, as well as Internet services (...), keep only the positioning and operational data, namely the technical data".

14. **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 is no such a provision.

15. **Please describe the applicable rules on reimbursement of costs in detail. Does the sentence "The amount of costs ... is determined as a sum of book depreciation items" (Art. 1 and 2 of Decree No. 486/2005) mean that the full costs are effectively reimbursed, but distributed to several years, according to book depreciation rules? Otherwise please explain how this is to be understood. How and by whom (government authority, provider) are the amounts to be reimbursed calculated? How are the specific data retention costs delimited against the costs for the general storage equipment and the general data storage process used in the context of service provision, billing and related business activities?**

    The amount of costs to be paid is determined as the sum of depreciation and direct and indirect costs incurred or related to the establishment and securing of the interface. Entitled to reimbursement of the costs of establishing and securing the interface created at the request of an authorized entity under § 7 of the Decree No 336/2005 Coll. on the form and extent of information provided from a database of publicly available telephone services and technical and operational conditions and for connecting the end points telecommunication equipment for interception and recording of messages. For the costs of setting up a security interface that was acquired after the effective date of this Order, an invoice will be sent to the authorized entity on whose application has been acquired by the interface. Invoice relating to the acquisition and security equipment designed for the retention of traffic and location data will be sent each month the Ministry of Interior. An invoice covering the cost of providing traffic and location data and providing information from a database of publicly available telephone services shall be sent for the month in which it was handled the request and it will pay for those beneficiaries who have requested data and information.

16. **Please give more details about how EU legislative acts and international treaties on cross-border co-operation in data retention issues (including rules specifically designed for data retention as well as general rules applicable to data retention) are applied in the Czech Republic.**

Act Nr. 101/2000 Coll. on the Protection of Personal Data and on Amendment to Some Acts in accordance with the law of the European Communities, international agreements binding the Czech Republic, and to exercise everyone's right to the protection from unauthorized interference with privacy, regulates the rights and obligations in processing of personal data and specifies the conditions under which personal data may be transferred to other countries.

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

    Police or other bodies entitled to obtain access to the data retained are subject to surveillance by the Office for the Protection of personal data under the Act No.101/2000 Coll., which is in this case subsidiary to the Bill on the Police (Nr. 273/2008 Coll.).This Office is an independent body.

18. **Please describe in detail how co-operation between the police and the other bodies entitled to request retained data according to Art. 78 para. 3 of the Act No. 273/2008 Coll. works: do the other bodies have to rely exclusively upon the data the police already have requested from the providers for their own purposes, or are they allowed to file a request on data access to the police, who will then in turn request these data from the provider and subsequently hand them over to the requesting body? If the latter is true: which requirements have to be fulfilled in each case in order for a body to be entitled to request that data be transferred from the provider to the police? Do the police have an own right to check the legality of such a request (over and above the general limit that a data transfer from the police to the requesting body may be denied if this would endanger the investigations carried out by the police)?**

    In accordance with the law on protection of personal data defining the basic classification schemes and legislation to personal data processing system according to the general regulations of the Law on personal data protection and for processing under the general provisions except in the case of processing for security purposes. (The purpose of the terminology into line with § 3, paragraph 6 of Act No. 101/2000 Coll. on the protection of personal data so that, inter alia, clearly stated the conditions under which the police are able to use exceptions to general rules of handling personal data.).

19. **According to your answer to question 15 of the first questionnaire, other purposes of use of the data retained may be defined by the law. Is there also a possibility to extend the group of bodies (or even private individuals) entitled to request the data?**

    "Other purposes of use" does not mean other persons or bodies entitled to request the data.

20. **According to your answer to question 26 of the first questionnaire, the provider has to develop technical and organisational rules which ensure "data protection**

and communications confidentiality with respect to the existing technical capabilities and the costs needed to provide protection at a level adequate to the risks of compromising the protection". Are the terms "existing technical capabilities" and "costs needed to provide protection at a level adequate to the risks of compromising the protection" further defined by law or jurisprudence? If so: please provide details on these definitions. If not: what is your understanding in general terms and with regard to some examples of how the meaning of these terms should be construed?

Above mentioned terms are not further defined by law, nor jurisprudence.

21. **Does "remote access" (as mentioned in Art. 3 para. 2 of the Decree No. 485/2005 Coll.) literally mean a direct access to the data or just a possibility to request and, subsequently, transfer the data remotely (i.e. by telecommunications means)?**

    It means the data should be requested and subsequently transferred. There is no direct access to the data.