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

Lithuania

Prof. Dr. Mindaugas Kiškis

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

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

I. Legal provisions

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

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

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

Yes, the provisions of the directive have already been fully transposed into national law through the Law on Electronic Communications (No IX-2135, April 15, 2004).

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

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

   Please refer to answer No 1.

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?**

   Please refer to answer No 1.

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.**

   Please refer to answer No 1.

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

General questions

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

   The English version of the Law on Electronic Communications is available but only without latest amendments. Please see the link below http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=242679 .

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

   The legislation amending the Law on Electronic Communications (No IX-2135, April 15, 2004), which transposed the Directive, was passed on November 14, 2008. It came into force only on March 15, 2009. Thus, the transition period continued for 4 months.

   In practice the transition was more than ten years, since first attempts to establish data retention in Lithuania were made in 1998. The article 27 part 2 of the Law on Telecommunications (adopted on June 9, 1998; amended July 11, 2000; later superseded by the Law on Electronic Communications) stated that telecommunications operators using their own funds and equipment must record all telecommunication events and participants, as well as maintain and ensure technical possibility for entities of operational activities to monitor the content of the information transmitted via telecommunications networks; also operators must

provide all this information for entities of operational activities free of charge when it is needed for the investigation or prevention of the criminal acts, according to the procedure and scope to be established by the Government.

The Constitutional Court of the Republic of Lithuania was asked to evaluate the constitutionality of the above provisions. In the ruling on the Law on Telecommunications (No IX-2135, April 15, 2004), Law on Operational Activities (IX-965, June 20, 2002), and the Code of Criminal Procedure (No IX-785, March 14, 2002) adopted on September 19, 2002, the Court concluded that:

– Electronic communication service and public connection network operators can be obliged to retain and provide data without any compensation, only as much as it is required for their own ordinary business activities.

– Any equipment and operating costs necessary for the fulfilment of this obligation beyond their own business discretion shall be compensated.

– Only the legislator shall establish the scope and procedures of data retention and provision thereof to entities of operational activities.

Thus the initial data retention regulations were effectively struck down on constitutional grounds. As it was noted The Law on Electronic Communications replaced the Law on Telecommunications on April 15, 2004, and amendments on data retention implementing the Directive were passed on November 14, 2008 (Law No. X-1835) and came into force as of March 15, 2009.

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.

The rules indicated in the Directive are transposed by the Act of Parliament (Law), i.e. the Law on Electronic Communications (No IX-2135, April 15, 2004). The maters regarding restriction of human rights are always dealt with by parliamentary legislation.

Corresponding to such kind of matters the Parliament adopts laws wherein

fundamental regulations are established. It is usual practice that laws do not concern all the technical and administrative matters, therefore more detailed regulations are established by the secondary legislation. Types of such legal acts may differ depending on the institution which implements the law (i.e. resolutions of the Government, orders of the Minister and legal acts of other executive bodies and institutions). It shall be noted that all secondary regulations must be in full compliance with the laws.

Only one part concerning the indication of authority, which is obliged to collect the information about data retention, is tackled by the Resolution of the Government on Authorization to Implement the Law on Electronic Communications (No 1593, December 6, 2004).

Furthermore, the Government has approved the description of technical data on electronic communications in public communications networks disclosure to competent authorities by the Government Resolution (No 1569, November 3, 2010), which came into force as of 15 November 2010. This description establishes order how providers of public communications network and (or) public electronic communications services shall disclose technical data on electronic communications in public communications networks to competent authorities (i.e. operational investigation services, pre-trial investigation institutions, prosecutor's office and courts). Also, technical requirements for data processing by automatic means equipment and request order are established.

In addition, the order of Director of the State data Protection Inspectorate on general requirements for organizational and technical measures (No 1T-71, November 12, 2008) provides the requirements for organizational and technical measures, which shall be put in place for safeguarding the data retained.

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

The terms *unsuccessful call attempt, cell ID* and *user ID* are transposed from the Directive and identically defined in the national law, while definitions of *data, user* and *telephone service* are not transposed.

The definition of *data* is not defined directly in the national law, but it is used in the same meaning in the Article 65 of the Law on Electronic Communications describing categories of data to be retained in general.

The term *user* is defined in the Law on Electronic Communications very closely to the Directives, however the purposes stated in the Directive "for private or business purposes, without necessarily having subscribed to that service" are excluded and not mentioned.

The term *telephone service* is not defined in the same way as the Directives. In the Law on Electronic Communications there is a definition *publicly available telephone services* which means the services available to the public for originating and receiving national and international calls and access to emergency services through a number or numbers in the National Telephone Numbering Plan, and in addition may include the following services: the provision of operator assistance, directory enquiry services, provision of public pay telephones, provision of service under special terms, provision of special facilities for customers with disabilities or with special social needs and/or provision of non-geographic services

The national law transposing the Directive indicates that terms used in the rules describing the processing[1] of electronic communication data, which are not defined in this law, are defined in the Law on Legal Protection of Personal Data (No I-1374, June 11, 1996), which transposed the Directive 95/46/EC. The terms transposed from Directive 95/46/EC *personal data, processing of data, controller, processor, third party, filing system* and *consent* are defined not identically, but the substantial meaning of them in the national law is generally the same.

The term *personal data* does not deviate in any way, except the structure which is adapted to Lithuanian language.

The term *processing of data is defined* similarly, but the specific operations with data are described as follows: collection, recording, accumulation, storage, classification, grouping, combining, alteration (supplementing or rectifying), disclosure, making available, use, logical and/or arithmetic operations, retrieval, dissemination, destruction or any other operation

In the terms *controller, processor, third party* the description of subjects does not mention such entities as "public authority, agency or any other body". Additionally to the term *processor* there is a statement that the data processor and/or the procedure of its/his nomination may be laid down in laws or other legal acts.

In the term *filing system* specific criteria is not described in the same way as in the directive and it refers to specific criteria relating to the person, allowing an easy access to personal data in the file.

The term *consent* additionally attaches statement that "consent with regard to special categories of personal data must be expressed clearly, in a written or equivalent form or any other form giving an unambiguous evidence of the data subject's free will".

In addition to the above, the Law on Electronic Communications (No IX-2135, April 15, 2004) is also transposing the Directives 2002/21/EC and 2002/58/EC.

---

[1] ***Data processing*** shall mean any operation, which is performed with personal data such as collection, recording, accumulation, storage, classification, grouping, combining, alteration (supplementing or rectifying), disclosure, making available, use, logical and/or arithmetic operations, retrieval, dissemination, destruction or any other operation or a set of operations.

The terms transposed from Directive 2002/21/EC *electronic communications network, public communications network, associated facilities, user, universal service, subscriber, provision of an electronic communications network, end-user, enhanced digital television equipment* and *application program interface (API)* are defined identically. The terms *transnational markets, national regulatory authority, Specific Directives* and *conditional access system* (term *conditional access* is defined) are not defined. The term *consumer* is defined similarly, but additionally noting family and household purposes for usage of services. The term *electronic communications service* is defined differently. It means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting (re-broadcasting). Electronic communications services exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services and do not include information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

The terms transposed from Directive 2002/58/EC, namely *call* and *electronic mail* are defined identically. The terms *user, communication* and *consent* are not defined. The terms traffic *data*, *location data* and *value-added service* are defined differently. *Traffic data* means any data processed for the purpose of the conveyance of a communication on an electronic communications network and/or for the billing thereof. *Location data* means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of an actual user of electronic communications services. *Value-added service* means, to the extent that it is related to the processing of personal data and the protection of privacy, any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.

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?

All the data, which have to be retained according the Directive, shall be retained according to the national law. The data categories defined in paragraph 5 of the Directive have been fully transposed to the Annex of the Law on Electronic Communications in identical structure ant the same content word by word. There are two categories of additional data, which go beyond the obligations mentioned in the Directive - namely the data on unsuccessful call attempts and location data resulting from the use of mobile email services. The obligation to retain these data has not existed before the Directive and related national acts were enacted.

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 national law does not rule out for the retention of communication data (customer records, traffic data and the content of communications). According to exception indicated in the Law on Electronic Communications (No IX-2135, April 15, 2004) retention of content of communication data is not prohibited, it must be justified by clear business needs or when motivated court decision based on Law on Operational Activities (IX-965, June 20, 2002), and the Code of Criminal Procedure (No IX-785, March 14, 2002) is adopted.

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

The data (categories defined in paragraph 5 of the Directive and fully transposed in the Law on Electronic Communication) retention is mandated only for the purpose of prevention, investigation, detection and prosecution of serious or very serious crimes. The Criminal Code (No VIII-1968, September 26, 2000) in the article 11 defines that the serious crime is an intentional crime, for which the gravest penalty of six to ten years imprisonment is applicable; the very serious crime is an intentional crime, for whose commitment the gravest penalty is of no less than ten years imprisonment.

12. **Are there any specific rules in national law prohibiting the retention and/or transmission of sensitive data (i.e. data that is legally considered to be particularly worthy of protection, e.g. data resulting from a communication between individuals that are in a relationship of mutual trust particularly protected by law for reasons of overriding importance, as might be the case between a lawyer and his/her client, between a doctor and his/her patient, between a journalist and a whistle-blower)?**

The national law does not specifically prohibit the retention and/or transmission of sensitive data. Though the Law on Legal Protection of Personal Data (No I-1374, June 11, 1996) in the Article 5 notes that it shall be prohibited to process special categories of personal data (data concerning racial or ethnic origin of a natural person, his political opinions or religious, philosophical or other beliefs, membership in trade unions, and his health, sexual life and criminal convictions), except in the following cases:
1) the data subject has given his consent;
2) such processing is necessary for the purposes of employment or civil service while exercising rights and fulfilling obligations of the data controller in the field of labour law in the cases laid down in laws;
3) it is necessary to protect vital interests of the data subject or of any other person, where the data subject is unable to give his consent due to a physical disability or legal incapacity;
4) processing of personal data is carried out for political, philosophical, religious

purposes or purposes concerning the trade-unions by a foundation, association or any other non-profit organisation, as part of its activities, on condition that the personal data processed concern solely the members of such organisation or to other persons who regularly participate in such organisation in connection with its purposes. Such personal data may not be disclosed to a third party without the data subject's consent;
5) the personal data have been made public by the data subject;
6) the data are necessary, in the cases laid down in laws, in order to prevent and investigate criminal or other illegal activities;
7) the data are necessary for a court hearing;
8) it is a legal obligation of the data controller under laws to process such data.

Thus retention of sensitive data is possible under the provision (6) above, which coincidentally is the general requirement for retention of any other data.

There are no specific regulations on retention of traffic and location data of communications potentially containing any sensitive data.

During the criminal procedure every person has a right to secrecy of his personal correspondence, telephone conversations, telegraph messages, and other communications, unless these rights are restricted by the procedure laid down in the Code of Criminal Procedure (No IX-785, March 14, 2002). Furthermore, the Code in the Article 154 part 6 states that it is forbidden to record and listen to conversations between the advocate and the suspect or the accused transmitted by electronic communications and it is forbidden to control, record or store any other data transmitted by electronic communications between them.

Additionally, sensitive data may be used as the evidence in a criminal case only if it meets the general requirement for evidence to be verifiable and legitimately obtained.

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

According to the Law on Electronic Communications (No IX-2135, April 15, 2004) data are retained for 6 months. There are no distinctions according to data categories.

The Article 72 part 2 in the Law on Electronic Communications sets the possibility that in cases where retained information is necessary for the purpose of prevention, investigation and detection criminal acts, this initial period may be extended by the order of entitled institution (operational investigation services, pre-trial investigation institutions, prosecutors, courts or judges), but for no longer than additional 6 months. The requirements for these orders are not expressly addressed hence general requirement to provide justification for such requests shall be followed.

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)?

Under present legislation neither any authority nor any bodies are entitled to directly access the data retained, except the provider of a public communications network and/or public electronic communications services as much as they need it for normal business purposes. Though, undertakings providing electronic communications networks and/or services shall allow competent authorities to access to retained data on their request upon providers in accordance with the procedure established by the legal acts. The procedure is set in the Description of description of technical data on electronic communications in public communications networks disclosure to competent authorities, which was approved by the Resolution of the Government (No. 1569, November 3, 2010). This description defines the term of the competent authorities which means the operational investigation services, pre-trial investigation institutions, the prosecutor's offices of the Republic of Lithuania and courts.

The term „operational investigation services" covers entities of operational activities defined in the Law on Operational Activities (No IX-965, June 20, 2002) and it refers to the Second Investigation Department under the Ministry of National Defence, the Financial Crime Investigation Service under the Ministry of the Interior, the Customs Department under the Ministry of Finance, the Police Department under the Ministry of the Interior, the Special Investigation Service, the VIP Protection Department under the Ministry of the Interior, the State Security Department, and the State Border Guard Service under the Ministry of the Interior. Thus intelligence services fall into this definition.

In addition, it shall be mentioned that providers of a public communications network and/or public electronic communications services shall disclose all retained data and other information which is available to them and which is necessary to prevent, investigate and detect criminal acts. According to the description retained data should be processed by automatic means and in cases where such technical possibilities are unavailable - in written form.

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

The data retained may be used only for the purpose of prevention, investigation, detection and prosecution of serious or very serious crimes (for the definitions of the crimes please refer to answer No 11).

The national law does not grant any specific rights to individuals to access the data retained directly. General access rights may be implied from the Law on Legal Protection of Personal Data, however the procedure for such access it is not clear

and there is no precedent of such access being granted so far.

According to the article 23 in the Law on Legal Protection of Personal Data (No I-1374, June 11, 1996) the data subject has a general right to have an access to his personal data and to be informed of how they are processed. This right means that the data subject presenting to the data controller or the data processor a document certifying his identity shall have the right to obtain information on the sources and the type of his personal data that has been collected, the purpose of their processing and the data recipients to whom the data are disclosed or have been disclosed for at least the last year.

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)?

There are no specific requirements for authorized institutions to access the data retained for purpose mentioned in answer No 15. The access to these data shall be guaranteed by order of the authorized institution or a sanction of the court.

In order to access the data competent institutions must make a request upon providers of a public communications network and/or public electronic communications services. The Description of data on electronic communications in public communications network disclosure to competent authorities sets main requirements for the content of such request. Therefore it must contain as follows:

- the legal grounds of the request;
- Identification data of public communications network terminal equipment (telephone network number, internet protocol (IP) address) and (or) other technical data on electronic communications possibly retained by the provider under which the data necessary for the investigation are requested;
- The period whereof technical data on electronic communications in public communications networks are requested to access;
- the signature of the authorised person.

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?

One of the possibilities to access the retained data is through obtaining a court order before accessing the data retained, though other institutions such as operational investigation services, pre-trial investigation institutions, prosecutors may also access the data retained upon a request to the providers of a public communications network and/or public electronic communications services in accordance of the procedure set by government. It is not required to hear the aggrieved party to involve him/her otherwise in the proceeding before data is accessed.

Scholars and observers have criticized the system for being too lax on access, i.e. in practice even the courts do not require substantial proof before granting access.

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 authorized institutions are allowed to use retained data only for the purpose of prevention, investigation, detection and prosecution of serious or very serious crimes; therefore the notification neither prior nor after the data access is obligatory. There no specific rules providing the notification of the aggrieved party.

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

Generally the aggrieved party shall be informed that data are processed (it is deemed automatic though in case of communications data retention), though the laws do not oblige to inform the aggrieved party about the data accesses.

Generally the aggrieved party presenting to the data controller or the data processor a document certifying his identity shall have the right to obtain information on the sources and the type of his personal data that has been collected, the purpose of their processing and the data recipients (Data recipients means a legal or a natural person to whom personal data are disclosed) to whom the data are disclosed or have been disclosed for at least the last year according to the Law on Legal Protection of Personal Data (No I-1374, June 11, 1996). Nevertheless, the State Data Protection Inspectorate and other state and municipal institutions and agencies shall not be regarded as data recipients when they obtain personal data in response to a specific request for the purposes of fulfilling their control functions laid down in laws.

The article 5 part 1 of the Law on Legal Protection of Personal Data (No I-1374, June 11, 1996) states that personal data may be processed if processing is necessary for the exercise of official authority vested by laws and other legal acts in state and municipal institutions, agencies, enterprises or a third party to whom personal data are disclosed. This law does not specify or expressly address to these functions- they are described in legal acts regulating appropriate institution's activities.

As a result, there is no obligation to inform the aggrieved party about accesses of the state and municipal institutions and agencies (including operational investigation services, pre-trial investigation institutions, prosecutors, courts or judges) and no effective right for such party to learn on access to his/her retained data. On the other hand there are not any prohibitions to inform the aggrieved party about the accesses by his/her request.

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

The aggrieved party does not have the recourse to courts for the data access, which

is made by authorized institutions for lawful purposes (Please refer to answer No 14). The aggrieved party in the case of an unlawful data access or processing operation has the right to complain to the State Data Protection Inspectorate, police, court with civil claim, prosecutor or the subject of pre-trial investigation institution (during the process of the pre-trial investigation).

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.

There are no specific legal provisions protecting the data retained against unauthorised access. There are only general legal provisions protecting the lawful data processing. It could be mentioned that the article 5 of the Law on Legal Protection of Personal Data (No I-1374, June 11, 1996) states cases where personal data may be processed:

- the data subject has given his consent;
- a contract to which the data subject is party is being concluded or performed;
- it is a legal obligation of the data controller under laws to process personal data;
- processing is necessary in order to protect vital interests of the data subject;
- processing is necessary for the exercise of official authority vested by laws and other legal acts in state and municipal institutions, agencies, enterprises or a third party to whom personal data are disclosed;
- processing is necessary for the purposes of legitimate interests pursued by the data controller or by a third party to whom the personal data are disclosed, unless such interests are overridden by interests of the data subject.

Any other data processing which contradicts these or other requirements shall be considered as unlawful.

In addition, the Law on Legal Protection of Personal Data *in article 30* (No I-1374, June 11, 1996) generally notes that the data controller and data processor must implement appropriate organisational and technical measures intended for the protection of personal data against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. These measures must ensure a level of security appropriate to the nature of the personal data to be protected and the risks represented by the processing and must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc.)

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

The operational investigation services shall destroy the personal information, which is not necessary for investigation after 3 months. Other authorized institutions may use the data as long as it is necessary for the access purposes, unless maximum retention period (6 months plus possible extension) is reached, or unless data is classified as evidence in which case it is retained until the lapse of the term of statutory limitations. For the criminal offence the terms of statutory limitations are

set in The Criminal Code of the Republic of Lithuania (No VIII-1968, September 26, 2000). The article 95 of the Code states that if the person who has committed a criminal act may not be subject to a judgement of conviction where the term of statutory limitations has lapsed:

- two years, in the event of commission of a misdemeanour;
- five years, in the event of commission of a negligent or minor premeditated crime;
- eight years, in the event of commission of a less serious premeditated crime;
- ten years, in the event of commission of a serious crime;
- fifteen years, in the event of commission of a grave crime;
- twenty years, in the event of commission of a crime relating to a premeditated homicide;

Moreover, there is a condition that during such period, the person must not hide from pre-trial investigation or a trial and must not commit a new criminal act.

Dimension 2 (State – economy)

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

The Law on Electronic Communications (No IX-2135, April 15, 2004) states that all private bodies/enterprises which provide electronic communications networks and/or services are obliged to retain the data. "Electronic communications services" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting (re-broadcasting). Electronic communications services exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services (such as internet news blogs) and do not include information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.

"Electronic communications network" means transmission systems and/or switching or routing equipment and other facilities which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including the Internet) and mobile terrestrial networks, electricity cable systems (to the extent that they are used for the purpose of transmitting signals), networks used for radio and/or television broadcasting (re-broadcasting), and cable television and microwave multi-channel distribution system networks, irrespective of the type of information conveyed. The examples of these bodies/enterprises may be internet service providers, cable television network providers, transmission providers, publicly available mobile/fixed telephone services providers, etc.

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 exceptions from the basic obligation to retain data. Thus, there are no parties who are exempt from these obligations.

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

The providers originally were entitled to retain the data, which was necessary for billing and other business purposes, as well as traffic data according to the Law on Telecommunications (adopted on June 9, 1998; amended July 11, 2000). Specific purposes were not set forth, however it was mentioned that personal data might have been processed for the call's establishment proposes and also for direct marketing purposes only after the data subject has given his consent.

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)?

The general provisions of the Law on Legal Protection of Personal Data (No I-1374, June 11, 1996) are applicable and hence general data processing diligence principles apply, such as adequate technical and organisational data protection measures, requirement of a formal written procedures, internal safeguards, etc.

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)?

The private persons, which are obliged to retain the data are mostly commercial entities, which do not report their expenditure publicly (or do not identify it as a separate line of expenditure), therefore there no available aggregate figures on the costs of the data retention before and after the implementation of the national law transposing the Directive.

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 costs of the obliged parties for retentions of the data are not reimbursed,

although the law sets forth a general rule that in case some specific equipment is needed (e.g. article 68 part 2 of The Law on Electronic Communications notes the equipment for the transferring location data to Emergency Response Center which is not necessary to ensure economic activities of obliged parties), then the costs may be borne by the state. We are aware that reimbursements are being made, but mainly this is the subject of the agreement between the authority and the obliged party.

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

The Law on Electronic Communications (No IX-2135, April 15, 2004) exclusively governs co-operation between the party retaining the data and the party (public authorities) accessing them. The article 66 part 1 of The Law on Electronic Communications states that providers of a public communications network and/or public electronic communications services must notify the State Data Protection Inspectorate about the data processed and generated in their networks in accordance with the procedure established by the Government. Furthermore, according to the article 61 of mentioned law providing electronic communications networks and/or services shall create conditions for the State Data Protection Inspectorate to exercise the control provided for in this paragraph in accordance with the procedure established by the Government.

In addition, it could be noticed that undertakings providing electronic communications networks and/or services shall designate persons to work with notices by operational investigation services on the use, in accordance with special procedure, of technical measures in their networks or to respond to enquiries by operational investigation services, pre-trial investigation institutions, prosecutors, courts or judges. Such persons must have security clearance and must be authorised to work with or have access to classified information in accordance with the procedure established by the Government.

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 Law on Electronic Communications (No IX-2135, April 15, 2004) provides economical sanction, which are monetary fines of up to 3 per cent of total annual income or altenatively from 10,000 to 300,000 LTL (approx. 2,860 EUR to 85,700 EUR).

In addition, the Communications Regulatory Authority shall have the right to impose economic sanctions for failure to provide information in accordance with appropriate provisions of the Law on Electronic Communications, without imposing the procedure established described above.

More generally, the Code of Administrative Law Infringements (as amended on July 10, 2010) provides fine up to 2000 LT (approx. 570 EURO) for unlawful processing of data, which may be applied to individual officers of a responsible party.

Therefore the State Data Protection Inspectorate issues statements of the offence according to which national courts may impose fines. The types of the infringements state in the Code are:

- processing personal data in contravention of the Law on Legal Protection of Personal Data (Article 214(14)) ;
- violation of the rights of the data subject established by the Law on Legal Protection of Personal Data(Article 214(16)) ;
- violation of the processing of personal data and the protection of privacy set by The Law on Electronic Communications. (Article 214(23)).

Also there are criminal sanctions such as fine, detention, imprisonment (up to 3 years) for breach of an individual's right to private life specified in the Criminal Code (No VIII-1968, September 26, 2000). These sanctions according article 167 of the Code could be imposed for unlawful collection of information about a person's private life by a court and it shall be noticed that legal entity shall also be held liable for such actions.

The civil liability compensation may be awarded according the Civil Code (No VIII-1864, July 18, 2000).

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?

According to the description of technical data on electronic communications in public communications networks disclosure to competent authorities by the Government resolution (No 1569, November 3, 2010) the State Security Department is responsible for the organization and implementation of the technical possibilities (i.e. installation and operation of the equipment and communication channels) to ensure competent authorities the access to the technical data on electronic communications in public communications networks.

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

No.

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

There are no specific rules governing the co-operation among the different bodies accessing the data indicated in the Directive. The authorized bodies share the

information on the basis of the need-to-access principle and in accordance with the Code of Criminal Procedure.

Need-to-access principle means that authorized bodies performs actions, access and exchanges appropriate information in cases where it is an absolutely necessary for the investigation, detection and prosecution of the criminal acts and justification is provided.

Moreover, there are special categories of criminal acts which are investigated not only by the general institutions, but also special entities of operational activities (e.g. money laundering, VAT embezzlement and other criminal activities against the State financial system are investigated by the Financial Crime Investigation Service, bribery and corruption-related offences – Special Investigation Service, etc.). Therefore these institutions shall be notified about specified crimes and data related to them shall be transferred to those institutions.

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)?

There are no specific rules governing the exchange of retained data indicated in the Directive with other EU Member States, other EEA Member States and third countries. The exchange of data is processed under general basis in accordance with the Code of Criminal Procedure (No IX-785, March 14, 2002) and international treaties. The Prosecutor General Office is responsible for cross-border data exchange. Supervisory role is assigned to the State Data Protection Inspectorate.

Most of the general rules for the procedure are contained in the Article 67 of the Code of Criminal Procedure. As to the procedure itself, the courts, prosecutors, pre-trial investigation institutions perform actions upon the request from foreign country's' institutions or international organizations, which they receive through the Ministry of Justice of the Republic of Lithuania or the Prosecutor General Office. In cases the request can not be fulfilled it is sent back in the same way as it was received. Thus the access to retained data and exchange of information should take place regarding these rules. However, it should be noted that performed actions must not contradict the Constitution, national laws and main principles of the criminal procedure.

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)?

Supervisory role in both technical advisability and legality is assigned to the State Data Protection Inspectorate. The article 36 of the Law on Legal Protection of Personal Data (No I-1374, June 11, 1996) states that the State Data Protection Inspectorate shall be a Government institution financed from the State budget and shall be accountable to the Government. But on the other hand the article 37 sets the rule that state and municipal institutions and agencies, members of the Parliament, other officials, political parties, public organisations, other legal and natural persons shall have no right to exert any kind of political, economic, psychological or social pressure or other illegal influence on the director of the State Data Protection Inspectorate, civil servants and employees employed under labour contracts. Interference with the activities of the State Data Protection Inspectorate shall entail liability in accordance with laws. There are further draft legal acts in the pipeline, which would ensure full legal independence of the State Data Protection Inspectorate.

Additionally, it shall be noted, however, that internal organizational controls within the institutions dealing with retained data (e.g. police, prosecutors offices) are in place.

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?

There are no lawsuits or administrative proceedings concerning the legality of the national law (Law on Electronic Communications) transposing the Directive at the moment. But there were proceedings in the Constitutional Court in 2002.

The Constitutional Court of the Republic of Lithuania in the ruling on the Law on Telecommunications (No IX-2135, April 15, 2004), Law on Operational Activities (IX-965, June 20, 2002), and the Code of Criminal Procedure (No IX-785, March 14, 2002) adopted on September 19, 2002. Content of the ruling is summarized in answer to Question No. 6 above.

Present legislation on reimbursements can be a subject of debate whether or not it is in line with the conclusions of the Constitutional Court, but further constitutional challenges are unlikely due to implementation of the European Union directive.

If so, please answer to the following questions:

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

The claimant was a group o the Seimas (Parliament of the Republic of Lithuania) members.

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

The subject of the challenge was the article 27 part 2 of the Law on Telecommunications (adopted on June 9, 1998; amended July 11, 2000), which stated that telecommunications operators using their own funds and equipment must record all telecommunication events and participants, as well as maintain and ensure technical possibility for entities of operational activities to monitor the content of the information transmitted via telecommunications networks; also operators must provide all this information for entities of operational activities free of charge when it is needed for the investigation or prevention of the criminal acts, according to the procedure and scope to be established by the Government.

The claimants stated that the challenged law was in conflict with the Article 22 of the Constitution of the Republic of Lithuania, which notes that the private life of a human being shall be inviolable; personal correspondence, telephone conversations, telegraph messages, and other communications shall be inviolable; information concerning the private life of a person may be collected only upon a justified court decision and only according to the law; the law and the court shall protect everyone from arbitrary or unlawful interference in his private and family life, from encroachment upon his honour and dignity.

As well as the conflict was with the Article 23 of the Constitution of the Republic of Lithuania, which notes that property shall be inviolable; the rights of ownership shall be protected by laws; property may be taken over only for the needs of society according to the procedure established by law and shall be justly compensated for.

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?

The Constitutional Court expressed an opinion that:

- Electronic communication service and public connection network operators can be obliged to retain and provide data without any

compensation, only as much as it is required for their own ordinary business activities.

- Any equipment and operating costs necessary for the fulfillment of this obligation beyond their own business discretion shall be compensated.

- Only the legislator shall establish the scope and procedures of data retention and provision thereof to entities of operational activities.

As a result, these unconstitutional rules were abandoned (not applied in practice). Please note that the principal concern of the Constitutional Court was not addressed at the heart of the newer data retention legislation.

Data retention regime in Lithuania is compatible with the requirements of the European Union which have been transposed, but there still are matters which are not expressly addressed in the laws. Such uncertainty leads into discussions and more specific legislations are needed to finish them.

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

There are no lawsuits with European courts concerning the legality of data retention obligations in which Lithuania is/was involved. Lithuania did not join on any side to the ECJ case on data retention.

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 centralized level?

The data are stored locally (not centralized) and at the service providers' premises equipment). External companies may be engaged as the data processors on contractual basis. Entities of operative activities are also expressly entitled to store the data themselves.

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

The data are stored by the obliged parties, which are network or services providers. These providers may be foreign entities. It is not formally prohibited to store data outside the country, and it may certainly be permissible under the data controller contractual arrangements. In addition, the company shall register as the data controller (or data processor) in the State Data Protection Inspectorate in order to

have the right to retain the data.

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

a) no data are retained beyond what is permitted?

The retaining persons are controlled by the State Data Protection Inspectorate, which is monitoring the data retention adequacy. In practice the control is rather limited, since the State Data Protection Inspectorate responds to complaints or conducts rather formal reviews of retention activities. There are no specific guidelines related to this issue and practical measures taken by the companies are their internal concern.

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)?

It is not a requirement of the law that a court order is a mandatory prerequisite for data access. The only safeguard in the Law on Electronic Communications (No IX-2135, April 15, 2004) is the formal request procedure, which requires that in order to get the data the authorized institutions shall provide justification. There are no technical interfaces enabling State bodies to access the data directly.

As it was noted in practice the access is relatively lax, and even the courts do not require substantial proof for wrongdoing when granting access.

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

The State Data Protection Inspectorate is entitled and obliged to monitor whether data are used for legitimate purposes or not. In practice the aggrieved persons has the right to complain to the State Data Protection Inspectorate and later to the court if he/she thinks that the data pertaining to them are not used for purposes other than those permitted. As mentioned in the part a) there are no specific guidelines related to this issue and practical measures taken by the companies are their internal concern.

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.

Again the State Data Protection Inspectorate is entitled and obliged to monitor

whether data are used for legitimate purposes or not. There are no other special institutions or specific rules concerning the matter. The general principles of organizational and technical measures are set forth in the order of the Director of the State data Protection Inspectorate on general requirements for organizational and technical measures (No 1T-71, November 12, 2008).

This order establishes general requirements for the organizational and technical measures which must be implemented by the data controller and processor for the protection of personal data against accidental or unlawful destruction, alteration and disclosure as well as against any other unlawful processing. Furthermore, this order sets 3 security levels for the data processing by the automatic means and provides a list measures which could be taken.

These measures must ensure a level of security appropriate to the nature of the personal data to be protected and the risks represented by the processing and must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc.).

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

Again the control is vested in the State data Protection Inspectorate, which is monitoring the data retention, as well as the destruction.

Although there are only general rules and there are no specific regulation for the guidelines of this matter, in practice the economic reasons and exponential growth of the amount of data regulate the providers and require them either to sustain ever increasing expenditure or to destroy retained data. Same applied to authorities, which have suffered massive budget cuts over the last couple of years.

Overall the destruction of data in not properly regulated beyond the general obligation.

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)?

Please refer to answer No 18.

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

Again the control is vested in the State data Protection Inspectorate, which is generally monitoring the data retention. As it was also noted, the aggrieved persons have the right to complain to the State Data Protection Inspectorate and later to the court.

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)?

My assessment is that the control of the data processing performed by the State Data Protection Inspectorate and performed by the internal data protection officers is not as effective as it should be. This is not because the lack of will, but rather to the lack of powers, staff and budget to support them.

The effective control mechanism is not described in any legal act. As to the role of the State Data Protection Inspectorate, this institution could be described as understaffed and underpowered. The State Data Protection Inspectorate is not a "power institution", while the "power institutions", especially the State Security Department have been extensively criticized as the "state within a state" and have been acting rather self-discretionally on many matters.

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

There are no obligatory technical standards, which are applied with respect to data retention and transmission. It is regulated on contractual basis.

No special provisions on interoperability are in place.

The obliged parties shall guarantee the safety of the data; hence they are tying to ensure the security standards according to the current technologies.

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.

In practice this is governed on contractual basis. Unfortunately the contractual rules are confidential.

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?

There is no specific cross-border transmission procedure regarding the data indicated in the Lithuanian laws. There is only one basic provision that data is shared on the grounds of international (or bilateral) treaties.

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).

The society is generally aware of the public surveillance. There were some public debates about this in late 2008, but is was mostly given up as the EU requirement.

The great majority of the citizens were against the surveillance, they believed it is infringement of the human rights, i.e. the right to privacy. The companies, which became the obliged parties, were against the surveillance as well, though because of increasing expenses.

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

No.

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.

Not available.

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?

Not publicly available.

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 discussion regarding reimbursement of the costs to obliged parties and exact scope of the data to be retained (especially content) is ongoing.

Currently there are no specific provisions requiring companies to a blanket retention of communications content.

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

The fundamental right to personal life is resulted from the Constitution and indicated in other legal acts and case-law.

According to the article 22 of the Constitution (English version may be found by the following link http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_l?p_id=275302) the private life of a human being shall be inviolable.

This right is not absolute and the protected scope may be reduced when it is legal obligation under laws to process or retain data. This is stated directly in the Constitution expressing that information concerning the private life of a person may be collected only upon a justified court decision and only according to the law.

Content of the fundamental right to personal life is described in the case law of the Constitutional Court. The court has declared that provisions of the article 22 of the Constitutions defend the right to privacy. This right covers private, family and domestic life, physical and mental inviolability of the person, dignity and reputation, the secrecy of personals facts, prohibition to announce confidential information and etc. Also the Constitutional Court has defined the private life of a human as personal life of individual: lifestyle, marital status, residential surroundings, relationship with other persons, convictions of the persons, habits, physical and mental state, honour, dignity and etc.

The definition of the private life in legislation is further elaborated in the Law on Provision of Information to the Public (No I-1418, July 2, 1996), wherein private life is defined as personal and family life of a person, his residential surroundings consisting of a person's dwelling, with its private territory and other private premises, which a person uses for his economic, commercial or professional activities, as well as mental and physical inviolability of a person, a person's honour

[2] 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).

and reputation, secret personal facts, a person's photographs or other images, personal health information, private correspondence or other communications, personal views, convictions, habits and other data which are allowed to be used only with his consent.

The telecommunication content is not explicitly defined in the national (constitutional) law. But the Constitution in the article 22 notes that personal correspondence, telephone conversations, telegraph messages, and other communications shall be inviolable as fundamental rights. The Constitution and the Law on Electronic Communications (No IX-2135, April 15, 2004) prohibits the retention of telecommunications content without a specific reason.

These regulations are in line with the provisions of the Constitution regarding freedom of expression and information. The article 25 states that freedom to express convictions, to receive and impart information may not be limited otherwise than by law, if this is necessary to protect the health, honour and dignity, private life, and morals of a human being, or to defend the constitutional order.

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?

Article 22 of the Constitution directly states that information concerning the private life of a person may be collected only upon a justified court decision and only according to the law. Restrictions to the fundamental right to personal life are possible in accordance with this article and general conditions to restrict human rights (i.e. restrictions must be established by the law only when they are necessary to guarantee the security of society, the public order, the health and morals of the people as well as other basic rights and freedoms of the person and they are proportional to their aims). The law transposing the Directive is also limiting this right by obliging to retain the data regarding communication.

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

There is no official opinion regarding the Directive or the laws implementing it. The Constitutional Court has expressed its opinion on similar matter in 2002, however this was later replaced by the new rules implementing the Directive. Although many aspects are similar, constitutionality of the law implementing the Directive was not questioned. Please also refer to answer No 36 for more information.

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?

No such discourse in the national (constitutional) law exists. Please also refer to answer No 52. Balance of different interests and fundamental rights affected by any data retention activities restricting a fundamental right is not elaborated in the jurisprudence or the case law. Overall it is not considered a fruitful constitutional law topic, due to prevailing attitudes of etatism among the Lithuanian constitutional law scholars.

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.

II. Dimension 2 (State – economy)

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

The retention obligations are clearly perceived as restricting the constitutional privacy rights. They are mostly understood as the EU imposed rules, which are only loosely in line with national (constitutional) law.

From time to time there are episodes of public or professional outrage about the retention of data pertaining to professional communication (especially communication involving Members of the Parliament, judges or advocates (legal counsels), since there are occasional leakages of such information to the media. On the other hand there is no clear understanding of the data retention and what it means for the public.

Overall, currently there are no significant debate about these rules and their limits among the legal scholars or the affected parties.

It shall be stressed again that obligated parties and the general public, as well as at least some legal scholars perceive national data retention rules transposing the Directive as restricting the fundamental rights of both the individuals, and the obligated parties. Nevertheless there is little willingness to step up and attempt to initiate any changes to the rules, or even to explore them in the scholarly work. Most expect that change shall come from the EU, which imposed the rules in the first

place.

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)?

Private actors currently do not play a role in law enforcement in Lithuania and have no access to the data retained. National law transposing the Directive does not set any general obligations for the private actors to assist the law enforcement for the purposes of data retention.

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

It is imperative to provide reimbursement of the obligated parties for the costs incurred according to national (constitutional) law, only as much as such costs are specific and pertain to data, which is not necessary for the business of the retaining (obligated) parties. The issue of such compensation is not hovewer clearly addressed in the law and remains vague. Generally, the obligated parties are unders strong pressure to retain data without compensation, as it was confirmed through private discussions with them.

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 European Convention on Human Rights is ratified and applicable directly. Generally ratified international treaties and conventions have superior power compared to the laws of Parliament, but according to the article 7 of the Constitution any law or other act, which is contrary to the Constitution, shall be invalid hence they rank below the Constitution. More directly all the ratified international treaties have the power of the law, and supersede over the provisions of law in case of conflicting provisions. The international treaties, which are not ratified, have the power of the power of the executive regulations, i.e. inferior to the laws.

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?

In order to transpose the Directive, the rules indicated in the Directive shall be transposed into the national legal act (usually law of Parliament). These amendments (containing new regulation) shall pass through all the legislative process. Under no circumstances the Directives are applicable directly, without the national implementation stage.

Lithuania as the member of European Union follows the case law of European Court of Justice. Also the principle of direct effect established by the European Court of Justice is applied and if there are all conditions fulfilled (i.e. the transposition deadline has fallen due or if the Directive was not transposed correctly and if the provisions of the directive are clear, sufficiently precise, and non-conditional) Directive may have direct effect. Moreover, it shall be noticed that the court of Lithuania interpret national legislation related to EU law transposition and implementation in accordance with the directives, if direct effect is not possible.

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 understanding of leading scholars and jurists in Lithuania is that the transfer of national sovereignties to the European Union is somewhat permissible as a result of the Lithuanian international obligations under the EU treaties and hence is roughly in line with the national (constitutional) law.

The Constitution *ex officio* doesn't express that national sovereignties could be transferred to the European Union. According to the Constitutional act of the Republic of Lithuania on membership of the Republic of Lithuania in the European Union the Republic of Lithuania as a Member State of the European Union shall share with or confer on the European Union the competences of its State institutions in the areas provided for in the founding Treaties of the European Union and to the extent it would, together with the other Member States of the European Union, jointly meet its membership commitments in those areas as well as enjoy the membership rights.

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 power regarding data retention is not divided among ministries and authorities, but mainly concentrated in the competence of the State Data Protection Inspectorate.

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

No specific limits are set forth.

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?

Clearly more detailed regulation on the data subject's rights are needed. According to their own words the retaining parties (ISPs, etc.) are more or less content with the situation, as they have resolved most issued with the authorities on contractual basis. Unfortunately, such resolutions remain largely unknown to the general public and may be contrary to the interests of the data subjects. Thus, more transparency and openness in the process would be desirable.

Clearer standards for access to the data retained are also needed. There is consistent and reasonable criticism of the system, that it has become almost automatic. The minimum burden of proof standard needs to be set for allowing access, either through case law or preferably legislation.

On the other hand in most cases contains only small part of data, which does not include content, but only includes the necessary information to identify the person using electronic networks or services, is retained in Lithuania, what is a certain protection in itself. Retaining parties have certain discretion here, and so far they are siding with the lesser retention. But in the absence of legislative safeguards, such situation is not warranted to last.

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

Lithuania

Prof. Mindaugas Kiškis

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*?

Not expressly. Article 22 of the Constitution provides that written communication, telephone conversations, telegraph communication and other communication of a person shall be inviolable.

In the jurisprudence it is interpreted as a right to privacy of communication, rather than anonymity of communication.

Other provisions of the Article 22 of the Constitution deal with other aspects of individual's privacy.

2. Please illustrate in detail any amendments to current data retention legislation that are presently discussed in your country (please also make reference to the issues mentioned in your answer to question 49 of the first questionnaire in this respect). How strong (in terms of support they get by the public) are the different arguments uttered in this context? Are the proposals for improvement set out in your answer to question 63 of the first questionnaire discussed in the public? If so: by which parts of society, and what degree of attention do they get in the public debate as a whole? Particularly: is the "quick-freeze" option, as foreseen by the Council of Europe's Cybercrime Convention (Art 16 para. 2), discussed as a potential alternative to data retention?

New amendments of the Law on Electronic Communication (No. XI-1522) were passed by the Lithuanian Parliament (Seimas) on June 28, 2011. They are not yet signed by the President, however are expected to be signed and promulgated.

Principal amendments pertaining to data retention refer ti strengthening of the role of the State Data Protection Inspectorate. Retaining entities are obliged to maintain an internal registry and rules for processing inquiries into retained data. Retaining entities shall submit information about inquiries, their number, provided data and legal background of the inquiries to the State Data Protection Inspectorate upon request. Retaining entities are made fully responsible for the safety of the retained information and accountable in this respect to the State Data Protection Inspectorate, which also gains powers to regulate data safety matters.

Overall, data retention issues are out of the public focus presently in Lithuania.

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?**

   The boundaries are not clearly defined. There is a general obligation to offer reasonable cooperation for public authorities in the detection, investigation and prosecution of criminal offences, also in cases of public security or where life is at risk. No special regulations, which would elaborate on this general obligation exists.

   Several high profile cases are currently on-going in the courts (pertaining to internet content (criminal and unauthorized) blocking obligations for the ISPs), albeit are at a rather early stages.

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?**

   Three distinct mentions pertaining to the rights of individuals to testify/to deliver evidence against themselves exist:

   1) Constitutional principle (Article 31 of the Constitution);

   2) Administrative (petty crime) procedure rules – right not to testify against family or close relatives (Article 276 of the Code of Administrative Violations); same may be implied from, but not expressly laid down, from the general rules of the criminal procedure (Code of Criminal Procedure);

   3) Attorney-Client privilege (Articles 5, 45 and 46 of the Law on Bar of the Republic of Lithuania).

These rules do not include any mention or reference to the national law rules transposing Directive 2006/24/EC on data retention (which were adopted much later than all of the above).

There is no absolute ban for data pertaining to the above rules from being retained or transmitted after it is retained.

Whether it is admissible for use as evidence in court is highly specific. Attorney-client privilege expressly disqualifies any data from attorney-client communication (even if it was retained and/or transmitted) to be used as evidence in court. On the other hand, although relatives are entitled to refuse to testify, there is no prohibition to produce data retained from their telecommunication as evidence (as long as it was obtained in accordance with the law).

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?**

   Data is stored by the communications service providers and/or by the entitled bodies themselves (after it is accessed), however no specific rules on this are available. Similarly no specific rules or list of measures that have to be taken by these bodies in order to safeguard data protection and data security are available. General principle that adequate technical and organizational security measures shall be adopted is applicable.

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.**

   No official statistics or other public information is available.

B. Country-specific questions

7. **Please give your own opinion on the constitutionality of the data retention regime in your country as a whole (i.e. with regard to all parties concerned, e.g. users as well as providers of electronic communications services).**

   Current rules on data retention in Lithuania in my opinion are not constitutional, at least as much as they are vague and lack detail on many important aspects. New amendments are step into right direction, however inadequate.

   From the user perspective data retention is simply a very non-descript governmental surveillance scheme. Most users are not too concerned about it, simply because the government lacks resources and competence to comb through the retained data (at least this is a common perception). Also, most people view it and the government conveniently tries to portray it as the EU imposed obligation, rather than a domestic policy.

From the electronic communications services perspective, their biggest concern is cost burden. Regardless of the deliberations on the contrary, the electronic communications services providers essentially bear the costs of data retention themselves (and obviously pass these costs onto the consumers). There are fears that data retention scheme will be expanded and that it will be used as a founding block for other similar schemes (e.g. obligations to filter certain content on the internet).

8. **As regards the ruling of the Constitutional Court on the constitutionality of data retention as in effect prior to the transposition of the Directive (see your answer to questions 36/52 of the first questionnaire):**

   - **Does the Constitutional Court 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 Constitutional Court does seek to strike a balance with respect of the right to privacy and invasion of privacy resulting from data retention and access of retained data by the authorities, however does not base it on the proportionality principle.

     For the sources on striking a balance the Constitutional Court refers to the ECHR Malone v. UK (1984) decision.

     The court emphasized that restriction of privacy is possible, however only through motivated court order or legislative act (rather than executive order or executive act), restriction is necessary for protecting the constitutional values and goals, as well as rights and liberties of other persons in the democratic society, and the constitutional proportionality principle is observed.

     The court does not elaborate on the application of proportionality principle, since in this specific case it has established that the first condition is not met.

   - **Does the court speak out in any way on the alleged violation of Art. 22 of the Constitution, or only as regards Art. 23 of the Constitution (cost reimbursement)?**

     The Constitutional Court established both the violation of the Art. 22 of the Constitution and Art. 23 of the Constitution.

     Violation of Art. 22 of the Constitution was established based on two aspects:

     1) requiring the communications service providers to retain more data, than it is necessary for their ordinary business activities, causes violation of Art. 22;

     2) allowing the government or other executive body to establish rules for (including scope of) data retention, is also not compliant with Art. 22.

Violation of Art. 23 of the Constitution was established based on lack of cost reimbursement rules.

9. **What considerations during the legislative procedure have led to the deviation between the Directive and the national law in terms of the data categories to be retained (i.e. the obligation to retain location data generated when using mobile e-mail services)?**

   Emergency response considerations are cited in *travaux préparatoires* for all location related data.

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

    No such rules are in place. Thus retention of the same data (e.g. by virtual mobile operators) is in principle possible. In practice it is sorted out through the agreements between network operator and the service provider.

11. **According to your answers to questions 28 and 57 of the first questionnaire, a general rule says that specific costs pertaining to data not necessary for the business of the retaining parties have to be reimbursed. Could you please specify the norm this obligation derives from? Are you aware of any *contractual agreements* between the authority (is this the State Data Protection Inspectorate?) and the obliged parties, or any *reimbursement practices* applied in the context of data retention?**

    If so, please describe the content of such agreements/the applied practices in detail. In which form and to which extent (completely, certain percentage of the full costs, lump sum, mere depreciation of book-entry items on tax return) are the costs reimbursed? 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?

    Parts 2 and 3 of Article 77 of the Law on Electronic Communications sets forth the compensation of specific costs pertaining to extended data retention and for data not necessary for the business of the retaining parties (content data).

    The fact of certain understandings or contractual agreements between the authorities (in this case it is not State Data Protection Inspectorate, but rather the State Security Department) and the retaining parties is a bit of a public secret. Nevertheless the contents of such arrangements are unknown and unavailable. The fact of existence of such understandings or contractual agreements has never been officially confirmed or denied.

    No public information on any reimbursement practices is available.

12. **Please give more details about where and how the data is stored (see your answers to questions 38 and 39 of the first questionnaire): Does Lithuanian law provide for rules on the transfer of personal data to third countries that correctly transpose the provisions laid down in Chapter IV of Directive 95/46/EC?**

    No detailed information on the retained data storage practices is available. Beyond the general obligations of data security, this issue is not regulated.

    Lithuanian law (specifically – the Law on Legal Protection of Personal Data) provides for the exact rules on the transfer of personal data to third countries that correctly transpose the provisions laid down in Chapter IV of Directive 95/46/EC. Moreover the Lithuanian transposition is rather strict and formal (e.g. use of the Model Clauses or transfer to Safe Harbour countries does not relieve the parties from obtaining the individual authorization for the transfer).

13. **Please explain the general principles of organisational and technical measures set forth in the order of the Director of the State Data Protection Inspectorate No 1T-71, November 12, 2008, and the content of any other guidelines specifying rules on data security with respect to storage and transmission, as far as they are applicable to data retention. Are these specifications binding or not for the bodies concerned?**

    In particular: do these principles/guidelines provide for rules in one or more of the following areas:

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

    - **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on the encryption algorithm to be used or on the safe custody of the crypto-keys)**

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

    - **access logging**

    - **secure (irreversible) deletion after expiry**

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

    - **secure data transmission (cryptographic security, postal delivery)**

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

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

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

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

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

The above referred rules are binding on all data controllers, including for the bodies concerned. Equally, they apply not specifically and not exclusively to the data retention case, but rather are general rules applicable to any data processing (whether in electronic communications or elsewhere).

The particulars listed are not regulated in the order of the Director of the State Data Protection Inspectorate No 1T-71, November 12, 2008. Such particulars are regulated (or at least are supposed to be regulated) in the internal documents of the bodies concerned, which are not publicly available.

14. **Please provide more details about data exchange with other countries (see questions 34 and 44 of the first questionnaire):**

- **Which EU legislative acts and international treaties on cross-border co-operation in data retention issues (including both rules specifically designed for data retention as well as general rules applicable to data retention) apply to your country?**

- **May data be accessed directly by the entitled bodies?**

- **As regards outgoing requests: which national authority would be responsible for establishing the contact with the foreign competent authority/the foreign provider in order to request the data?**

From the point of view of the Lithuanian law, it is very difficult to establish the list of EU legislative acts and international treaties on cross-border co-operation in data retention issues, which are applicable to Lithuania. Our review did not point to any specific treaties or documents, which would expressly address exchange of information obtained through data retention. A lot of general treaties on legal assistance or cooperation in crime fighting activities are in place, but they do not deal specifically with cross-border co-operation in data retention issues. It is conceivable, however, that information and evidence obtained from data retention is transferred according to these treaties.

Generally the State Data Protection Inspectorate would be responsible for coordinating and supervising data exchange with other countries, however specific agreements or regulations may appoint different authorities to exercise this.

15. As regards your answer to question 35 of the first questionnaire:

- **Does the State Data Protection Authority also have the competence to monitor compliance of the providers with the data retention obligations, as far as these obligations do *not* refer to the protection of personal data? If not: which bodies are responsible for this task? Are these supervisory bodies independent in the sense of what has been said in question 35 of the first questionnaire?**

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

State Data Protection Inspectorate has no competence to monitor compliance of the providers with the data retention obligations, as far as these obligations do not refer to the protection of personal data. Such competence is partially vested in the Communications Regulatory Authority and partially in the State Security Department (as the coordinator of the operative activities pertaining to data retention). These latter bodies are reasonably independent.

Unfortunately there are there no external bodies responsible for supervising that the bodies entitled to obtain access to the data retained act within the law. Generally the courts are supposed to carry such supervision, when evaluating the evidence submitted. Very limited public control is exercised by human rights organizations.

According to the newest amendments of the Law on Electronic Communications the State Data Protection Inspectorate will gain powers to check the legal grounds for access to retained data. It is unclear yet how this is going to work in practice and who will be held responsible in case of violations. Secondary legislation is expected to establish more specific rules.