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

Republic of Latvia

LL.M. Aldis Kalinks

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 transposed into national law

- ***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)?

Not applicable.

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?**

   Not applicable.

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.**

   Not applicable.

- ***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 Electronic Communications Law with the last amendments made on July 1, 2009 is available at:

   http://www.ttc.lv/advantagecms/LV/meklet/meklet_dokumentus.html?query=electronic%20communications%20law&resultsPerPage=10.

   The recent wording of the law with the amendments made on July 14, 2010 is not currently available in English. Some regulation regarding the data retention existed in the Electronic Communications Law already before the Directive was enacted.

   The Regulations of the Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" is available at :

   http://www.ttc.lv/export/sites/default/docs/LRTA/MK_Noteikumi/Cab._Reg._No._820_-_Electronic_Communications_Transfers_Data_to_be_Retained.doc.

   The Criminal Procedure Law is available at:

   http://www.ttc.lv/export/sites/default/docs/LRTA/Likumi/Criminal_Procedure_Law.doc.

The regulations of the Criminal Procedure Law with respect to disclosure of the data stored in an electronic information system have existed also before the Directive was enacted.

The Investigatory Operations Law with the last amendments made on October 13, 2005 is available at:

http://www.ttc.lv/advantagecms/LV/meklet/meklet_dokumentus.html?query=Investigatory%20Operations%20Law&resultsPerPage=10. The recent wording of the law with the amendments made on November 8, 2007, April 22, 2009, and January 1, 2010 is not available in English. The regulations of the Investigatory Operations Law with respect to investigatory acquisition of information from technical means have existed also before the Directive was enacted.

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

   The relevant regulations which have been adopted or amended to transpose the Directive have been in force since the following dates:

   The relevant regulations of the Electronic Communications Law have been in force since June 8, 2005 with the amendments by enacting the Directive made on June 7, 2007.

   The Regulations of the Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" have been in force since December 8, 2007.

   The relevant regulations of the Criminal Procedure Law have been in force since October 1, 2005 with the amendments by enacting the Directive made on February 4, 2010.

   The relevant regulations of the Investigatory Operations Law have been in force since January 13, 1994 with the amendments by enacting the Directive made on January 1, 2010.

   There are no valid transition periods in place regarding the application of these regulations.

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 types of legal acts chosen for the different matters regulated correspond to those usually chosen in Latvia for such kind of matters. Please see answer b) below.

The Electronic Communications Law is adopted by the Parliament of the Republic of Latvia. The law determines the competence, rights and duties of users, electronic communications merchants, private electronic communications network owners and state administrative institutions, which are associated with the regulation of the electronic communications sector, the provision of electronic communications networks and the provision of electronic communications services, as well as the use and administration of scarce resources.

The Criminal Procedure Law is adopted by the Parliament of the Republic of Latvia. The law determines the order of performance of the criminal procedures that ensures the effective application of the norms of the Criminal Law. The Criminal Procedure Law also determines the procedure of the performance of the investigatory actions which includes the disclosure and issue of the data retained.

The Regulations of the Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" are adopted by the Cabinet of Ministers of the Republic of Latvia. These Regulations define the procedures according to which pre-trial investigative institutions, bodies performing investigatory operations, state security institutions, the office of the Prosecutor and court request and electronic communications merchant transfers data retained. The regulations also define the procedures and volume in which the Data State Inspectorate compiles statistical information regarding the requests to receive data retained from the authorities and regarding the issuing of data retained.

a) Issues which affect fundamental basic principles of one particular field are regulated with the laws adopted by the Parliament of the Republic of Latvia, whereas issues which define more precisely or specify the procedure of the realization of the fundamental basic principles of particular field are regulated by the regulations of the Cabinet of the Ministers of the Republic of Latvia.

b) The types of the legal acts mentioned above enacted to transpose the Directive correspond to those which are usually used to regulate such issues in Latvia.

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 following terms are defined in the Electronic Communications Law:

   "User" –means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service; in accordance with the Electronic Communications Law "user" is a natural person or legal entity, which **requests** or utilizes publicly available electronic communications services. Thereby, the „user" in accordance with the national legislation is also a person who has requested the electronic communications services.

   "Telephone service" – "telephone service" means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services). The term "telephone service" in the Electronic Communications Law is defined with two terms "voice telephony service" – a public electronic communications service, which ensures the transmission of a voice signal between electronic communications networks or electronic communications network termination points connected to electronic communications terminal equipment within a real time scale; and with term „electronic communications service" – a service that is usually ensured for remuneration and which wholly or mainly consists of the transmission of signals in electronic communications networks. The voice telephony service refers only to the transmission of the voice signals but electronic communications service refers to all signals transmitted in the electronic communications network.

   "Data" – The Electronic Communications Law defines each data type separately: traffic data, location data and data to be retained. **Traffic data** – any information or data, which is processed in order to transmit information by an electronic communications network or to prepare accounts and register payments, except the content of transmitted information. **Location data** – data, which is processed in an electronic communications network and indicates the location of the terminal equipment of an electronic communications service user. For public mobile electronic communications networks, satellite networks and non-wire networks, which are utilised for the distribution of radio or television signals, it shall be the geographic co-ordinates or address of the terminal equipment of an electronic communications service user, but for public fixed networks, cable television and cable radio networks, and electricity cable systems to the extent that they are utilised in order to transmit electronic communications signals – the termination point address. **Data to be retained** – the traffic data, location data and the associated data thereof, which is necessary in order to identify the subscriber or user.

The following terms are not defined within the national laws:

"User ID"

"Cell ID"

"Unsuccessful call attempt".

The national laws also define the following terms mentioned in the Directive 95/46/EC, Directive 2002/21/EC and Directive 2002/58/EC:

"Personal data" – any information related to an identified or identifiable natural person;

"Processing of personal data" – any operations carried out regarding personal data, including data collection, registration, recording, storing, arrangement, transformation, utilisation, transfer, transmission and dissemination, blockage or erasure;

"Personal data filling system" defined in the Personal Data Protection Law as **"Personal data processing system"** – a structured body of personal data recorded in any form that is accessible on the basis of relevant person identifying criteria;

"Controller" defined in the Personal Data Protection Law as **"System administrator"** – a natural person or a legal person, State or municipal institutions which determine the purposes and the means of processing of a personal data processing system and are responsible for the processing of the personal data in accordance with the laws;

"Processor" – a person authorised by a system administrator, who carries out personal data processing upon the instructions of the system administrator;

"Third person" – any natural person or legal person, except for a data subject, a system administrator, a personal data operator and persons who have been directly authorised by a system administrator or a personal data processor.

"Recipient" – a natural or a legal person to whom personal data are disclosed.

"The data subject's consent" – a freely, unmistakably expressed affirmation of the wishes of a data subject, by which the data subject allows his or her personal data to be processed in conformity with information provided by the system administrator and in accordance with the law.

"Conditional access system" defined in the Electronic Media Law as **"Conditional access control"** – a device, software or other solution that allow to receive the service only to authorized users;

"Consumer" defined in the Consumer Rights Protection Law, the term is defined in general, not with respect to electronic communications services – a natural person who expresses a wish to purchase, purchases or might purchase, or use goods or a

service for a purpose, which is not related to his or her economic or professional activity;

"Electronic communications network" – transmission systems, switching and routing equipment and other resources, which irrespective of the type of transmitted information permits the transmission of signals utilising wires, radio waves, optical or other electromagnetic means in networks, including: a) satellite networks, fixed networks (channel and packet switching networks, including Internet) and mobile terrestrial electronic communications networks, b) networks, which are utilised for radio and television signal distribution, and c) cable television and cable radio networks, electricity cables systems to the extent that they are utilised in order to transmit signals;

"Electronic communications service" – a service that is usually ensured for remuneration and which wholly or mainly consists of the transmission of signals in electronic communications networks;

“Public communications network" defined in the Electronic Communications Law as **“Public telephone network“** – an electronic communications network, which is utilised to provide voice telephony services, as well as the provision of other services (including facsimile information and data transmission) between public electronic communications network termination points;

"Associated facilities" – equipment or facilities, which are associated with an electronic communications network or electronic communications services and which allow or support the provision of services through the referred to electronic communications network or electronic communications services (including with the assistance of limited access systems and electronic programme guides);

"Universal service" – the minimum volume of electronic communications services with a specified quality, which for an affordable price is accessible to all existing and potential users irrespective of the geographical location thereof;

"Subscriber" – a natural person or legal entity who or which has entered into a contract with an electronic communications service provider regarding the receipt of specific electronic communications services;

"Provision of an electronic communications network" – the establishment, development, operation, control and provision of access to an electronic communications network;

"End-user" – an electronic communications services user who does not utilize such services to ensure electronic communications services to other persons;

"Enhanced digital television equipment" – set-top boxes, which are intended for connection to televisions or integrated digital televisions and which may receive digital interactive television services;

"Application program interface (API)" – the software interface with which broadcasters or electronic communications service providers ensure access to enhanced digital television equipment for digital television or digital radio services;

"Call" – a connection or attempted connection, which is performed utilising electronic communications services, which allows two-way communication in real time;

"Value added service" – a service, for the provision of which it is necessary such traffic data or location data processing, which exceeds the volume of data processing that is necessary for the provision of electronic communications services and to register payments;

"Electronic mail" – the type of the service which for the users of the computers added to the electronic communications network ensures the possibility to send and receive the announcement.

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?**

   In accordance with the Electronic Communications Law electronic communications merchants have to retain exactly the same data which are defined in the Directive – traffic data, location data and the associated data, which are necessary in order to identify the subscriber or user.

   The Electronic Communications Law states that also data on attempted connection should be retained.

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

    The Electronic Communications Law states that bodies performing investigatory operations may connect to electronic communications networks in order to obtain investigatory information and investigatory wiretapping of conversations in the cases specified by law. The procedure by which an electronic communications merchant installs in the electronic communications network equipment, which ensures the acquisition of this investigatory information is regulated by the Regulations of the Cabinet of Ministers No. 591 "Procedure by which an electronic communications merchant installs in the electronic communications network, equipment, which shall ensure the acquisition of investigatory information from technical facilities and the investigatory wiretapping of conversations in the cases

specified by law". The Criminal Procedure Law states that the control of telephones and other means of communications without the knowledge of the members of a conversation or the sender and recipient of information shall be performed, based on a decision of an investigating judge, if there are grounds for believing that the conversation or transferred information may contain information regarding facts included in circumstances to be proven, and if the acquisition of necessary information is not possible without such operation. In accordance with the Investigatory Operations Law investigatory covert monitoring of non-public conversations (including by telephone, by electronic or other means of communication) shall be performed only in accordance with the special method and with the approval of the Chief Justice of the Supreme Court or a Justice of the Supreme Court specially authorized by him or her.

In accordance with the Criminal Procedure Law a person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by the law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system. The duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days.

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

In accordance with the Electronic Communications Law data are retained in order to transfer them to pre-trial investigation institutions, persons performing investigative field work, state security institutions, the office of the Public Prosecutor and the courts pursuant to their request. The data retained are transferred to mentioned institutions for the purposes stated in the Clause 71.1 of the Electronic Communications Law - in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings.

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

In accordance with the Criminal Procedure Law sworn advocate has an immunity and it is prohibited to control the information systems and means of communication to be used by sworn advocate for the provision of legal assistance, to take information from such systems or means, and to interfere in the operation thereof.

In accordance with the Investigatory Operations Law it is prohibited to purposefully obtain, through investigatory operations measures, information at the time

professional assistance is being provided by sworn advocates, sworn notaries, doctors, teachers, psychologists and clergy, except in cases when there are sufficient basis to suspect such persons of planning or committing a criminal offence or threatening interests of importance to the state, or such persons are being sought with respect to a criminal offence already committed.

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 therefore.**

In accordance with the Electronic Communications Law data retained have to be kept for 18 months, except:

a) the data which have been requested by the respective institutions up to the end of the time period for the retention of data but which have not been issued yet;

b) the data, which are necessary for the provision of further services, payment accounting for services provided, the examination of claims, recovery of payments or ensuring interconnections.

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

The data retained are transferred to pre-trial investigation institutions, persons performing investigative field work, state security institutions, the office of the Public Prosecutor and the courts. The traffic data are transferred to the Public Utilities Commission, Data State Inspectorate. The location data are transferred to the State Fire-Fighting and Rescue Service, State police, emergency medical care and the gas emergency services, Maritime Search and Rescue Service or the number "112" service, as well as the Electronic Communications Office. The other institutions and persons may receive the data retained only if the electronic communications merchant has received the written consent from the user or subscriber whose data the respective institutions and persons request.

In accordance with the Clause 70 Part 8 of the Electronic Communications Law, in order to perform the supervision functions stated in the laws in the field of electronic communications, personal data protection and in the field of circulation of information society services the Data State Inspectorate has the rights to request and the electronic communications merchant has an obligation to provide the Data State Inspectorate with the traffic data within 15 days. In accordance with the Clause 70 Part 7 of the Electronic Communications Law the Public Utilities Commission (the Regulator) has the rights to request and receive from the electronic communications merchants, information regarding traffic data for the purposes of examination of the disputes or interconnection issue. The other institutions mentioned above receive retained data under the Clause 48 Part 2, the Clause 71 Part 7 and the Clause 711 Part 1 of the Electronic Communications Law.

Please note that the recent wording of the Electronic Communications Law is not available in the English. The Part 8 of the Clause 70 of the Electronic Communications Law was adopted in July 14, 2010, these amendments to the law is not available in the English.

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

In accordance with the Cause 71.1 part 1 of the Electronic Communications Law which was amended to transpose the Directive, the data retained which are transferred to pre-trial investigation institutions, persons performing investigative field work, state security institutions, the office of the Public Prosecutor and the courts are used to protect state and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings. In accordance with the Clause 70 Part 7 of the Electronic Communications Law the traffic data which are transferred to the Public Utilities Commission are transferred for the purpose of examination of disputes arising from the relations involved in the provision of public utilities or interconnection issues. In accordance with the Clause 70 Part 8 of the Electronic Communications Law the traffic data which are transferred to the Data State Inspectorate are used by the Data State Inspectorate in order to perform the supervision functions stated in the laws in the sphere of electronic communications, personal data protection and in the sphere of circulation of information society services. In accordance with the Clause 48 Part 2 and the Clause 71 Part 7 of the Electronic Communications Law the location data transferred to the State Fire-Fighting and Rescue Service, State police, emergency medical care and the gas emergency services, Maritime Search and Rescue Service or the number "112" service, as well as the Electronic Communications Office are used for the performance of the duties and the functions of these institutions.

In accordance with the Clause 70 Part 3 of the Electronic Communications Law the traffic data may be used by the electronic communications merchants for payment accounting regarding the electronic communications services provided, recovery of payments, examination of objections or provision of interconnections. In accordance with the Clause 70 Part 4 of the Electronic Communications Law the traffic data may be used by the electronic communications merchants for the distribution of electronic communications services and provision of value added services if the user or subscriber to whom such data relates has given written consent in accordance with the electronic communications services contract. In accordance with the Clause 71 Part 1 of the Electronic Communications Law the location data may be used by the electronic communications merchants to ensure the provision of electronic communications services. For other purposes data retained may be used by receiving the written consent of a user or subscriber.

In accordance with the other national law - the Clause 1 of the Investigatory Operations Law, data which are acquired in accordance with the Investigatory Operations Law from the electronic information systems are used to protect life and health, rights and freedoms, honor, dignity and property of persons and the safeguarding of the Constitution, the political system, national independence and territorial integrity, the capabilities of the State regarding defense, the economy, science and technology, and State official secrets, against external and internal threats. The operational data acquisition from the electronic information systems is one of the investigatory measures and in accordance with the Clause 4 Part 4 of the Investigatory Operations Law investigatory operations measures can be initiated and performed only if achieving the objectives determined before are not possible by other means or are significantly more difficult.

The national law does not allow individuals to access the data retained and the data retained cannot be used within the civil proceedings, except if the electronic communications merchant receives a written consent of the data subject (subscriber or user). This conclusion results from the Clause 71.1 of the Electronic Communications Law, which states that the data retained are transferred in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings. In accordance with the principle of the public rights - everything that is not allowed is prohibited, therefore, if the Electronic Communications Law allows using the data only in criminal proceedings, it is not allowed to use retained data in any other proceedings.

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)?

In order to access the data retained for the purpose to protect state and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings the threats against State and public security and the actual possibility that a criminal offence has taken place should exist.

In accordance with the Investigatory Operations Law, the data retained may be accessed in order to perform the following duties: 1) protecting of persons against criminal threats; 2) preventing, deterring and detecting of criminal offences, and the determining of persons committing criminal offences and the sources of evidence; 3) searching for persons who, in accordance with procedures prescribed by law, are suspected of, have been accused of or have been convicted of committing a criminal offence;4) ensuring compensation for damages resulting from a criminal offence; 5) searching for missing persons; 6) obtaining, accumulating, analyzing and utilizing, in accordance with procedures prescribed by law, of political, social, military, economic, scientific and technical, criminal, and other information related to the criminal sphere and its infrastructure, and threats against State security, defense and economic sovereignty; 7) the protecting of State secrets and other interests important to the State, and, in cases prescribed by law, the providing of special protection to persons; and 8) gathering of information about specific persons, if decisions must be taken regarding their suitability for work in important State

offices and for authorities, or regarding persons who have access to State secrets or other secrets protected by law. The process of the operational data acquisition from the electronic information systems is stated in the Clause 9 Part 5 of the Investigatory Operations Law. The Clause 9 Part 5 of the Investigatory Operations Law states that the operational data acquisition from the electronic information systems is the acquisition of such data which retention is stated in the law and which do not disclose the content of information expressed or kept by the person. The acquisition of retained data can be performed by receiving the consent of the director of the institution of the bodies performing the investigatory operations or consent of his authorized person. Please note that the recent wording of the Investigatory Operations Law is not available in the English. Part 5 of the Clause 9 of the Investigatory Operations Law was adopted in January 1, 2010, these amendments to the law is not available in the English. Before amendments the legal base of acquisition retained data was Clause 9 Part 1 (investigatory inquiry) of the Investigatory Operations Law not Clause 17 Part 2.

The operational data acquisition from the electronic information systems is one of the investigatory measures and in accordance with the Investigatory Operations Law investigatory operations measures can be initiated and performed only if achieving the objectives determined before are not possible by other means or are significantly more difficult. In order to fulfill the duties mentioned before data retained may be accessed before criminal proceedings are initiated, during the period of investigation of a criminal matter and continue after termination thereof. The provision to consider whether the objectives determined before are not possible to achieve by other means relates also to necessity to consider whether the actions can not be performed in accordance with the Criminal Procedure Law. In accordance with the Clause 4 Part 3 of the Investigatory Operations Law investigatory operations measures, and the manner, scope and intensity of the conducting thereof, must correspond to the form and danger level of the threat. Investigatory tasks shall be conducted so as to interfere as little as possible in the field of human rights. The law does not state that in order to perform the acquisition of data retained there should exist seriuous crime but it is necessary to evaluate whether the chosen investigatory measure correspond to the danger level of the threat.

The Investigatory Operations Law does not determine any other specific requirements for accessing the retained data.

In accordance with the Electronic Communications Law the Public Utilities Commission, Data State Inspectorate, the State Fire-Fighting and Rescue Service, State police, emergency medical care and the gas emergency services, Maritime Search and Rescue Service or the number “112” service, as well as the Electronic Communications Office may access data in order to fulfill the functions mentioned in the laws (see question 15). With respect to these institutions national laws do not determine any other specific requirements that have to be fulfilled in order to access the data retained.

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

It is not required to obtain a court order before accessing the data retained. In accordance with the Criminal Procedure Law in order to request data retained from the electronic communications merchant during the pre-trial criminal proceedings investigator should receive the consent of a public prosecutor and a public prosecutor should receive the consent of a higher-ranking prosecutor. During the pre-trial criminal proceedings investigator and a public prosecutor may requested data retained also by receiving the consent of a data subject. When adjudicating a criminal case data retained are requested by a judge or the court panel. These provisions are legal obligations which are stated in the Clause 192 of the Criminal Procedure Law.

In accordance with the Investigatory Operations Law in order to request data retained bodies performing the investigatory operations should receive the consent of the director of the institution of the bodies performing the investigatory operations or consent of his authorized person.

Except as stated in the Criminal Procedure Law, when during the pre-trial criminal proceedings investigator and a public prosecutor may requested data retained also by receiving the consent of a data subject, in the other cases the national law does not require to hear/involve aggrieved party in the proceedings before the data is accessed.

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

In accordance with the Electronic Communications Law an electronic communications merchant does not have the right to disclose the information regarding the fact that the data retained has been requested by or transferred to the respective institutions, as well as the information regarding users or subscribers in relation to whom data to be retained has been requested or transferred. There are no exceptions to this principle defined

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

No the aggrieved party does not have a right to be informed (see question 18).

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?

In accordance with the Electronic Communications Law an electronic communications merchant must ensure the retention of data retained in such volume

as they are acquired or processed in providing electronic communications services, as well as ensuring the protection thereof against accidental or unlawful destruction, loss or modification, or processing or disclosure. The Personal Data protection Law defines the rights of the aggrieved party to request that the processing of the personal data be suspended or that the data be destroyed if the personal data are processed unlawfully. The law also grants the rights to the aggrieved party to submit the complaint about the unlawful data procession to the Data State Inspectorate, which has the rights to impose administrative penalties regarding violation of the personal data processing. In accordance with the Personal Data Protection Law and Civil Law the aggrieved party has the rights to apply to the court in order to request the commensurate compensation if the person has suffered harm or losses by unlawful data procession. The aggrieved party has also the rights to submit the application about the unlawful data access or processing operation to the investigative institutions or to the Office of the Prosecutor.

The aggrieved party may take action against both – the electronic communications merchant and the prosecutor and/or investigator. But in accordance with the Office of the Prosecutor Law a prosecutor for committed administrative violations can be punished only disciplinarily. It does not exclude the rights of the agrieved party to request compensation in the civil proceedings or submit application within the criminal proceeding.

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.

In accordance with the Electronic Communications Law an electronic communications merchant must ensure the retention of retained data in such volume as they are acquired or processed in providing electronic communications services, as well as ensuring the protection thereof against accidental or unlawful destruction, loss or modification, or processing or disclosure. These provisions are stated in the Clause 711 Part 2 of the Electronic Communications Law.

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

In accordance with the Clause 16 and Clause 10 of the Personal Data Protection Law the data have to be destroyed when they are no longer necessary for the purposes for which they were collected but it should be taken into account that in accordance with the law it is allowed to use the personal data for the purposes other than those originally intended in the criminal matters in the following cases: 1) to prevent, detect, investigate crime and to perform the criminal prosecution or the execution of criminal penalties; 2) to use the personal data in the administrative or civil proceedings, as well as in the work of the authorized officers of the state institutions, if it relates to crime prevention, detection, investigations or criminal prosecutions, or enforcement of the criminal penalty; 3) to prevent immediate serious threat to public safety; or 4) if the data subject has given consent for data processing.

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.

In accordance with the Electronic Communications Law the data retention must be performed by the electronic communications merchants. In accordance with the law electronic communications merchant is a merchant or branch of foreign merchant, which has the rights to perform commercial activities, who ensures a public electronic communications network or provides electronic communications services in accordance with the Electronic Communications Law. A person who is the owner of the private electronic communications network (electronic communications network, which is established and is operated only to ensure the needs of the owner thereof) is not considered as an electronic communications merchant and therefore is not obligated to retain data. This conclusion results from the definition of „electronic communications merchant", which states that electronic communications merchant is a merchant who ensures a public electronic communications network or provides electronic communications services. The Clause 25 Part 2 of the Electronic Communications Law states that it is prohibited to provide electronic communications services by utilising a private electronic communications network. Therefore the owner of the private electronic communications network is not considered as an electronic communications merchant. Taking into account that in accordance with the Clause 711of the Electronic Communications Law only electronic communications merchant has an obligation to transfer the retained data to the authorized institutions, private communication network owners has no obligation to retain data.

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

No there are not anybody 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?

In accordance with the Electronic Communications Law the electronic communications merchants retained traffic data and location data before the Directive entered into force.

The Electronic Communications Law (law wording from 09.11.2006. – 06.06.2007, before the Directive was enacted) stated that the electronic communications merchant has an obligation to retain traffic data for the period of three years and to ensure transfer of the traffic data to the State Police, State security institutions and Corruption Prevention and Combating Bureau pursuant to their request. The law did

not specify the purpose for the data retention and transfer directly but it was planned to adopt the Regulations of Cabinet of Ministers where to state the purpose for retention and transfer of traffic data and data categories. The Regulations of Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" was adopted only in December 4, 2007, that is, after the Directive was enacted in the law. But taking into account that the legal provisions regarding the data retention and transfer were in force in Criminal Procedure Law and Operational Investigatory Law, the purposes of the data retention and transfer resulted from these both laws. The retention and transfer of the data in accordance with the Criminal Procedure Law was mandated for the purposes to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings and in accordance with the Operational Investigatory Law the retention and transfer of the data was mandated for the purposes stated in the Clause 1 of the Operational Investigatory Law (please see question 15).

In accordance with the Electronic Communications Law (law wording from 09.11.2006. – 06.06.2007) electronic communications merchants had an obligation within the limits of technical possibility, to ensure the specification of the location of the caller and the transfer of such data to the Electronic Communications Office.The Electronic Communications Office had an obligation to ensure the processing, maintenance and further transfer of data regarding the caller location received from electronic communications merchants to the State Fire-Fighting and rescue service, State Police, State security institutions, Corruption Prevention and Combating Bureau, emergency medical care, gas emergency service and the number "112" service. In accordance with the law the location data were data which were processed in an electronic communications network and indicated the geographical location of the terminal equipment of an electronic communications service user (address, geographical coordinates).

The Electronic Communications Law also permitted electronic communications merchants to use the traffic data for payment accounting regarding the electronic communications services provided, recovery of payments, and examination of objections or provision of interconnections; to use the traffic data for the distribution of electronic communications services and provision of value added services pursuant to written consent of the user or subscriber to whom such data related; to use the location data in order to ensure the provision of electronic communications services.

In order to use the data for the other purposes electronic communications merchants had to receive a written consent of a user or subscriber.

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 Personal Data Protection Law states that a system administrator and personal data processor have a duty to use the necessary technical and organizational measures in order to protect the personal data and to prevent the illegal processing. A system administrator must ensure that the personal data processing takes place with integrity and lawfully; the personal data is processed only in conformity with the intended purpose and to the extent required; the personal data are stored so that the data subject is identifiable during a relevant period of time, which does not exceed the time period prescribed for the intended purpose of the data processing; and the personal data are accurate and that they are updated, rectified or erased in a timely manner if such personal data are incomplete or inaccurate in accordance with the purpose of the personal data processing. In accordance with the Personal Data Protection Law all State and local government institutions, and other natural persons and legal persons which carry out or wish to commence carrying out personal data processing should register personal data processing in the Data Sate Inspectorate. Instead of registering the personal data procession in the Data State Inspectorate processor can appoint the personal data protection specialist who organizes, controls and supervises the procession of the personal data compliance with the laws.

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)?**

In accordance with the annotation of the national law transposing the Directive the implementation of the law did not affect the State budget. The information about costs of the private bodies originated from the transposing the Directive into the national laws is not publicly available.

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 obligated parties do not receive reimbursement for their costs.

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

Regulations of the Cabinet of Ministers No. 820 “Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled”. Regulations of the Cabinet of Ministers No. 1013

„Regulations regarding the Specification, Processing, Maintenance and Further Transfer of Data Regarding Caller Location". Please see question 43.

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.

Administrative liability

In accordance with the Clause 146.5 of the Latvian Administrative Violations Code for not providing the information stated in the laws for the location information database or for knowingly providing false information a fine shall be imposed to the legal persons in an amount from 500 – 2`000 LVL. In the case of the same activity, if recommitted within a year of the administrative sanction being applied fine shall be imposed to the legal persons in an amount from 1`000 – 5`000 LVL.

The location information data base existed before the Directive was enacted. The data base contains the location data. In accordance with the Regulations of Cabinet of Ministers No. 1013 "Regulations regarding the Specification, Processing, Maintenance and Further Transfer of Data Regarding Caller Location" the following information must be maintained in the data base: the telephone subscriber's number; the address of connection point or geographic coordinates in accordance with the address register of State Land Service; number of public pay telephone and location address or geographic coordinates in accordance with the address register of State Land Service; the location data of caller terminal equipment or geographic coordinates in accordance with the address register of State Land Service; identification data of the caller's terminal equipment and if the subscriber identification module or another identification module is used, also a subscriber's or caller's number.

The Latvian Administrative Violations Code Clause 204.7 defines that in the case of the illegal operations with a natural person's data a warning shall be issued or a fine shall be imposed to the natural persons in an amount from LVL 50 up to LVL 400, to officials – from LVL 100 up to LVL 400, but to the legal persons – from LVL 1000 up to LVL 8000, with or without confiscation of the articles and tools used to commit the violation. In the case of the illegal operations with a natural person's sensitive personal data a warning shall be issued or a fine shall be imposed to the natural persons in an amount from LVL 200 up to LVL 500, to officials – from LVL 300 up to LVL 500, but to the legal persons – from LVL 3000 up to LVL 10 000, with or without confiscation of the articles and tools used to commit the violation. In the case of the blocking of a natural person's data, failure to follow an order regarding deletion or destruction of incorrectly or illegally obtained data, as well as of continuing to process a natural person's data after a permanent or temporary prohibition on processing has been specified – a fine shall be imposed to the natural persons in an amount from LVL 50 up to LVL 500, to officials – from LVL 200 up to LVL 500, but to the legal persons – from LVL 1000 up to LVL 10 000.

Criminal liability

The Clause 144 of the Criminal Law defines that for a person who commits intentional violation of the confidentiality of personal correspondence or information in the form of transmissions over a telecommunications network, or commits intentional violation of the confidentiality of information and programs provided for use in connection with electronic data processing, the applicable sentence is deprivation of liberty for a term not exceeding three years or community service, or a fine not exceeding fifty times the minimum monthly wage, with or without deprivation of the right to engage in specific activities for a period not exceeding five years. For a person who commits the same acts, if such are committed for purposes of acquiring property, the applicable sentence is deprivation of liberty for a term not exceeding three years or community service, or a fine not exceeding one hundred times the minimum monthly wage, with or without deprivation of the right to engage in specific activities for a period not exceeding five years.

The Clause 245 of the Criminal Law states that for a person who commits violation of provisions regarding information storage and processing, which have been formulated in accordance with an information system or the protection thereof, or violation of other safety provisions regarding computerized information systems, where committed by a person responsible for compliance with these provisions, if such has been a cause of theft, destruction or damage of the information, or other substantial harm has been caused thereby, the applicable sentence is deprivation of liberty for a term not exceeding two years, or community service, or a fine not exceeding forty times the minimum monthly wage.

The Clause 145 of the Criminal Law defines that for a person who commits unlawful actions with the personal data if as a result the significant harm has been caused, the applicable sentence is deprivation of liberty for a term not exceeding two years or custodial arrest or community service or a fine not exceeding hundred times the minimum monthly wage. For a person who commits unlawful actions with the personal data for the purpose of acquiring property, revenge or blackmail if the person is personal data processor or operator, the applicable sentence is deprivation of liberty for a term not exceeding four years or custodial arrest or community service or a fine not exceeding hundred and twenty times the minimum monthly wage. For a person who has influenced a personal data processor or operator by using violence or threats or by use of trust in bad faith, or by deceit (fraud) with the purpose to perform unlawful activities with the personal data, the applicable sentence is deprivation of liberty for a term not exceeding five years or custodial arrest or community service or a fine not exceeding two hundred times the minimum monthly wage.

In accordance with the Personal Data Protection Law and Civil Law the aggrieved party has the rights to apply to the court in order to request the commensurate compensation if the person has suffered harm or losses by unlawful data procession.

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?

In accordance with the Regulations of the Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" each entitled body by itself establish the contact with the electronic communications merchant by submitting the request to the electronic communications merchant, in which the legal basis, volume, type and the term for the providing of a response for the request of data retained are indicated. The head of the authority assigns officials who are authorized to request the data to be retained and an electronic communications merchant are notified regarding the authorized officials. The electronic communications merchant also assigns persons who ensure the transfer of data retained to the entitled body.

Regarding the location data which are stored in the location information database the Electronic Communications Office is the institution which has an obligation to maintain the database and ensure for electronic communications merchants and operational services accessibility to a database for transfer and receipt of the required information for twenty four hours a day with a probability of accessibility of 0.999 per year (a database may be unavailable for one hour and twenty six minutes within a year).

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 there are no any regional entities vested with own authority that have been granted their own rights of access to the retained data.

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

The co-operation among the different bodies accessing the data and other public authorities in general are regulated by the Administrative Procedure Law, the State Administration Structure Law, the Criminal Procedure Law, the National Security Law, the Law on Prevention Money Laundering and Terrorism Financing, the Law on State Security Institutions, the Law On Police, the Investigatory Operations Law. The general rules have not been adapted in the course of the Directive's

transposition. As regards the exchange of the retained data between the different bodies there are no legal rules in place governing this co-operation. The general rules governing co-operation between public authorities defines that institutions co-operate in order to perform their functions and tasks. Institutions may co-operate both in individual cases and continuously. When co-operating continuously, institutions may enter into interdepartmental agreements. Public persons may also enter into co-operation contracts in order to achieve a more effective performance of the task that is within the competence of at least one contracting party – public person. An institution may refuse to co-operate, by substantiating the refusal in writing, if:1) co-operation is impossible due to practical reasons; 2) co-operation is impossible due to legal reasons; 3) another institution may be involved in the co-operation with less expenditure of resources; or 4) the necessary expenditure of resources exceeds the necessity of the institution that proposed the co-operation for such co-operation.

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

The exchange of retained data with EU Member States, EEA Member Sates and third countries are regulated by the Criminal Procedure Law, Conventions and international treaties. Foreign state bodies cannot access the retained data directly. The Minister for Justice has the rights to receive a request from the foreign state for criminal-legal co-operation, except if otherwise stated in the particular international treaty. The Minister for Justice is responsible for fulfillment of the request or transferring to the institutions which have the competence to fulfill the request. Except if otherwise stated in the particular international treaty, the Minister for Justice and General Prosecutor have the rights to submit the criminal-legal co-operation requests to other EU Member States. Please see question 44.

Even though the international treaties do not directly point out the exchange of retained data, there is a view that if the international treaties regulate the international cooperation in criminal matters and cooperation in investigative actions these agreements relate also to the exchange of retained data. The major international treaties which concern to the exchange of retained data are the following: Convention on Cybercrime, November 23, 2001; United Nations Convention against Transnational Organized Crime, November 15, 2000; International Convention for the Suppression of Terrorist Bombings, December 15, 1997; International Convention against the taking of hostages, December 17, 1979.

Latvia has also concluded bilateral agreements on legal assistance and legal relations in civil, family, employment and criminal matters with the EU countries - Estonia, Lithuania, Poland, and third countries- Belarus, Kyrgyzstan, Russia, Moldova, Ukraine, Uzbekistan. In accordance with these agreements the parties

have agreed to cooperate also in criminal matters which include cooperation in performance of the procedural actions. Taking into account that the procedural actions include also investigative actions, that is, also transfer of retained data, these agreements can be a legal basis for the exchange of retained data. The agreements do not state the procedure or order of transfer of exchange data directly but the agreements have general rules regulating the cooperation in performance of the procedural actions which could refer also to exchange of the retained data. These rules state the form, content and language used in the criminal-legal co-operation requests, institutions responsible for fulfilling the requests, etc. The general principle of the performance of the criminal-legal co-operation requests is that the laws of the recipient state (the state which receives request) are applicable in the performance of the requests. The recipient state should apply the laws of the requesting state (state which submits request) pursuant to its claim if it is not in conflict with the laws of recipient state.

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)?

In accordance with the Electronic Communications Law the Data State Inspectorate is the institution which supervises the protection of personal data in the electronic communications sector. The Data State Inspectorate is supervised by Ministry of Justice. The supervision applied is limited to the control of legality - the rights to examine the lawfulness of decisions and to revoke unlawful decisions, as well as to issue an order to take a decision in case of unlawful failure to act.

The Data State Inspectorate was also the supervisory institution with respect to personal data protection in the electronic communications sector before the Directive was enacted.

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?

No publicly available information about any lawsuits.

If so, please answer to the following questions:

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

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

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

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

No publicly available information about any lawsuits.

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

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

There is not any specific regulation which defines the data storage. In practice data can be stored at the service providers' premises or with the external companies. Generally the data are stored locally. The location data which are stored in the location information database are stored with the State.

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

The national law does not prohibit the data storage outside the Latvia. In accordance with the Personal Data Protection Law the national law applies in cases when the system administrator is registered in Latvia and the equipment for data procession is located in the territory of Latvia, except in cases if the equipment is used only for transmission of the personal data to other countries. Thereby, if the data are only transmitted through Latvia and processed and stored in the other country the national law is not applicable.

The companies involved in the data storage are considered as the personal data processor. The personal data system administrator must conclude an agreement with the personal data processor. In accordance with the Personal Data Protection Law the personal data processor has an obligation to process the personal data entrusted to him within the amount determined in the contract concluded with the system administrator and in conformity with the purposes provided for therein and in accordance with the instructions of the system administrator if they are not in conflict with regulatory enactments. Prior to commencing the personal data processing, a personal data processor must perform safety measures determined by the system administrator for the protection of the system.

Personal data may be transferred for storage to another state which is not EU or EEA states, if that state ensures such level of data protection as corresponds to the relevant level of the data protection in effect in Latvia, except if the system administrator undertakes to perform supervision regarding the performance of the relevant protection measures by concluding the agreement with respective company abroad, and at least one of the following conditions is complied with: 1) the data subject has given consent; 2) the transfer of the data is necessary in order to fulfill an agreement between the data subject and the system administrator, the personal data are required to be transferred in accordance with contractual obligations binding upon the data subject or also, taking into account a request from the data subject, the transfer of data is necessary in order to enter into a contract; 3) the transfer of the data is required and requested, pursuant to prescribed procedures, in accordance with significant state or public interests, or is required for judicial proceedings; 4) the transfer of the data is necessary to protect the life and health of the data subject; or 5) the transfer of the data concerns such personal data as are public or have been accumulated in a publicly accessible register. The Ministers of the Cabinet shall adopt regulations stating the compulsory provisions which should be included in the agreement concluded between system administrator and the company abroad. Till adoption of these regulations system administrators should take into account the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission.

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

a) no data are retained beyond what is permitted?

The Personal Data Protection Law states that a system administrator and personal data processor have a duty to use the necessary technical and organizational measures in order to protect the personal data and to prevent the illegal processing. In accordance with the Regulations of the Cabinet of the Ministers No. 40 “The compulsory technical and organizational requirements for protection of personal data” the data processor should adopt the internal rules of the protection of the data processing where the data processor should define the procedure of the personal data processing and the responsible person for the protection of the personal data, in such manner ensuring that the personal data are processed only in conformity with the intended purpose and to the extent required. These provisions are the obligations of the data processor.

There is not available an English version of the Regulations of the Cabinet of the Ministers No. 40 “The compulsory technical and organizational requirements for protection of personal data”.

In the Public Report of the Data State Inspectorate for year 2009 was mentioned that the Data State Inspectorate had ascertained that approximately 80 state and municipal institutions which had submitted audit report to the Data State Inspectorate (in accordance with the Personal Data Protection Law these institutions must submit one audit reports within two years to the Data State Inspectorate) had not adopted appropriate internal rules of the protection of the

data processing or other documents required by the law.[1] There is not publicly available information regarding the implementation of the internal data protection rules by other persons.

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

There are no technical interfaces enabling State bodies to access the data directly.

In accordance with the Regulations of the Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" entitled authorities, the Office of the Prosecutor and court must ensure the evaluation of the necessity and proportionality of the requests to the electronic communications merchant for data retained and performance of activities specified within laws to justify the request (to receive the consent of a public prosecutor or consent of a higher-ranking prosecutor); registration of the requests, identifying the authorised official who requested the data, the official who proposed the request of data to be retained, as well as the number of the particular criminal case or of the investigatory operation's process case in the scope of which the data retained are being requested; registration of the received data retained, indicating the official to whom the received data have been transferred.

In accordance with the Regulations of the Cabinet of the Ministers No. 40 "The compulsory technical and organizational requirements for protection of personal data" the system administrator must ensure that only authorized persons can access the personal data.

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

In accordance with the Regulations of the Cabinet of the Ministers No. 40 "The compulsory technical and organizational requirements for protection of personal data" the data processor should determine in the internal rules the obligations, restrictions and responsibilities of the users of personal data, ensuring that the personal data are processed only in conformity with the intended purpose.

---

[1] http://www.dvi.gov.lv/par_mums/dvi_parskats_2009.pdf, page 90-91.

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

The data processor has an obligation to indicate in the internal rules the personal data processing organizational procedures, defining the data processing time, place and procedures; means for the protection of the technical resources against intentional damage and unauthorized acquisition; media storage and destruction procedures; password length and password structure conditions; password usage procedures as well as the period after which the password should be changed; action if the password or crypto key become known to another person; rights, obligations, restrictions and responsibilities of the users of personal data. In accordance with the regulations the data processor must ensure that only authorized persons can access the personal data and technical resources that are used for data processing and data protection; that the media containing personal data are recorded, moved, arranged, transformed, transferred, copied or otherwise processed by the authorized persons; that only the authorized person performs the personal data collection, recording, the recorded data arrangement, retention, copying, overwriting, alteration, amendment, deletion, destruction, archiving, backup, locking, as well as provides the possibility to determine the personal data, which were processed without authorization, as well as processing time and the person who did it; that the resources used in processing of personal data are transferred by authorized persons; ensure that the following information are retained when transferring the personal data: data transfer time; the person who transferred the personal data; the person who received the personal data; the personal data being transferred. The data processor ensures that the following information is retained when receiving the personal data: the time receiving the personal data; the person who transferred the personal data; the person who received the personal data; information about the personal data. These obligations are stated in the Regulations of the Cabinet of the Ministers No. 40 "The compulsory technical and organizational requirements for protection of personal data".

In accordance with the Regulations of the Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" the head of the entitled body assigns officials who are authorized to request the data to be retained and an electronic communications merchant are notified regarding the authorized officials by sending it the necessary contact information (the given name, surname, position, address, telephone number, fax, e-mail). The electronic

communications merchant also assigns persons who ensure the transfer of data retained to the entitled body. The entitled bodies, the Office of the Prosecutor and court are notified regarding the authorised officials, by sending them the necessary contact information (the given name, surname, position, address, telephone number, fax, e-mail).

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

In accordance with the Regulations of the Cabinet of the Ministers No. 40 "The compulsory technical and organizational requirements for protection of personal data" the data processor should determine in the internal rules the personal data processing organizational procedures and media storage and destruction procedures. The data processor should also appoint persons who are responsible for information resources, technical resources and protection of personal data and determine their rights and responsibilities.

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

Notification is not provided in the law.

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

In accordance with the Regulations of the Cabinet of the Ministers No. 40 "The compulsory technical and organizational requirements for protection of personal data" the data processor should determine in the internal rules the obligations, restrictions and responsibilities of the users of personal data and define the procedure of the personal data processing and transmission, in such manner ensuring that the sensitive data are not retained or transmitted.

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)?

In accordance with the Regulations of the Cabinet of Ministers No. 40 "The compulsory technical and organizational requirements for protection of personal data" the personal data processor has an obligation to perform internal personal data procession audit and to prepare a report on the measures taken in the field of protection of the information. In accordance with the Personal Data Protection Law State and local government institutions have an obligation to submit to the Data State Inspectorate a personal data processing system internal audit findings every year (also a system risk analysis) and a report regarding measures performed in the field of information security. In accordance with the Personal Data Protection Law the Data State Inspectorate has the rights to perform the inspections of a personal data processing to verify if the data procession is performed in accordance with the laws.

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?

Latvian Standard LVS EN 1047-2:2010 Secure storage units - Classification and methods of test for resistance to fire - Part 2: Data rooms and data container. There is no publicly available information regarding the operational systems used with respect to data retention and transmission by private bodies. The electronic communications merchants have the rights to freely choose the operational systems and standards to be applied.

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 accordance with the Regulations of the Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" the data retained are requested by an authorized officials of the pre-trial investigative institutions, bodies performing investigatory operations, State security institutions or the Office of the Prosecutor, or court by sending a request to the electronic communications merchant, in which the legal basis, volume, type and the term for the providing of a response for the request of data retained are indicated.

The respective authorities, the office of the prosecutor and court may also enter into a contract with a electronic communications merchant regarding electronic exchange of data retained. If the parties have concluded the contract a request may also be sent electronically. Requirements regarding encoding of information and identification of persons, conditions for the security of data retained and for issuance of information in matters of urgency, as well as the obligations of the parties are provided in such contract.

An electronic communications merchant shall ensure submission of the data retained within the following time periods after the receipt of a request:

1. within 30 days, if data requested were retained more than six months ago;

2. within 10 days, if data requested have been retained during the last six months;

3. in matters of urgency, if the transfer of data within the time period mentioned above may hinder the prevention or disclosure of a criminal offence, saving a person's life or protection of the State or public safety– within three hours, if the data requested have been retained within a time period of the last twenty-four hours or within an hour for particular type of data.

In accordance with the Public report of the Data State Inspectorate for year 2009, the Data State Inspectorate had inspected 24 electronic communication merchants and recognized that there is not unified legal framework and unified established internal procedures for issuing the data retained to authorized institutions.2There are not any other publicly available information regarding the practice of process and method of data transfer.

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?

In accordance with the Criminal Procedure Law a request for criminal-legal co-operation is submitted in writing, if an international agreement has not specified otherwise. A request shall indicate: 1) the name of the authority of the submitter of the request; 2) the object and essence of the request; 3) a description of the criminal offence and the legal classification of such offence; 4) information that may help identify a person. The Minister for Justice is responsible for fulfillment of the request or transferring to the institutions which have the competence to fulfill the request.

A request for criminal-legal co-operation must be written and submitted in the official language, a translation in the language of the relevant state must also be attached to a request. If the criminal-legal co-operation is regulated by the international treaty the sates attach the translation of the request into the language agreed in the agreement. If an international agreement does not determine a language of communication, a request may be submitted to a foreign state without attaching a translation. A competent institution may come to an agreement with the competent institution of a foreign state regarding a different procedure for language use.

[2] http://www.dvi.gov.lv/par_mums/dvi_parskats_2009.pdf. Page 40.

B. National (societal) context

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

There was an active discussion between Ombudsman, the Ministry of Justice and the Office of the Prosecutor regarding the necessity of the court control over the transmission of the data retained to the authorized institutions. The opinion of the Ombudsman was that the transmission of the data retained to the institutions restricts the rights to inviolability of private life and correspondence. The rights to the private life and the rights to inviolability of the correspondence are not absolute and can be restricted in accordance with the Constitution of the Republic of Latvia if the restriction is stated in the law and necessary in order to protect the rights of other people, the democratic structure of the State, and public safety, welfare and morals. Therefore the Ombudsman indicated that in order to recognize that the restriction is necessary in the democratic society it is obligated to provide the control of the court over the transmission of the data retained.[3] The Ministry of Justice and the Office of the Prosecutor admitted that the data requested from the electronic communications merchant do not disclose the content of the communication and thereby the data received do not significantly infringe the fundamental rights of persons, therefore the request to transmit the data in accordance with the Investigatory Operations Law should be performed in accordance with the general methods not the special method by receiving the approval of the Chief Justice of the Supreme Court. Also the respective legal norms of the Criminal Procedure Law were enacted by the initiative of the Ministry of the Justice and now state that it is obligated to receive the consent of a public prosecutor or consent of a higher-ranking prosecutor not consent of the court. There was also a discussion about whether the data retained should be transmitted to the authorized institutions in the case of investigation of criminal offences (crimes and criminal violations)[4] or only crimes. The Ombudsman and the electronic communications merchants indicated that data transmission is

---

3 http://www.tiesibsargs.lv/lat/petijumi_un_viedokli/viedokli/?doc=199.

4 In accordance with the Criminal Law the criminal offences are criminal violations and crimes. A criminal violation is an offence for which the Criminal Law provides deprivation of liberty for a term not exceeding two years, or a lesser punishment. A crime is an intentional offence for which the Criminal Law provides for deprivation of liberty for a term exceeding two years till a term exceeding ten years or life imprisonment.

proportional with the restriction of the fundamental rights only in cases of investigation of the crimes. However the position of the law enforcement institutions was that data retained is necessary for investigation of all criminal offences.[5]

Lawyers pointed out the positive and negative effects of the directive. In general lawyers admitted the positive and advisable effect of the Directive. The negative aspect mentioned by lawyers was additional costs for electronic communications merchants for obtaining the equipment for providing data retention and transmission. The positive aspect mentioned was the adoption of the shorter period for the retention of the data.[6]

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. In accordance with the Personal Data Protection Law personal data processing is permitted only if at least one of the following conditions exist:1) the data subject has given his or her consent; 2) the personal data processing results from contractual obligations of the data subject or, taking into account a request from the data subject, the processing of data is necessary in order to enter into the relevant contract; 3) the data processing is necessary to a system administrator for the performance of his or her duties as specified by law; 4) the data processing is necessary to protect vitally important interests of the data subject, including life and health; 5) the data processing is necessary in order to ensure that the public interest is complied with, or to fulfil functions of public authority for whose performance the personal data have been transferred to a system administrator or transmitted to a third person; and 6) the data processing is necessary in order to, complying with the fundamental human rights and freedoms of the data subject, exercise lawful interests of the system administrator or of such third person as the personal data have been disclosed to.

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.

No, there are no publicly available statistics.

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?

No there is no publicly available information.

---

5 http://www.juristavards.lv/index.php?menu=DOC&id=167629.

6 http://rln.lv/en/publications/Saldo%20Nr.12_08_2006_GL.pdf

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?

There are discussions going on regarding the use of the data retained in the civil cases, especially in cases where the honor and dignity of the person has been affected in the internet.[7]

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

The national fundamental rights which protect privacy, personal data and the secrecy of telecommunications are the rights to inviolability of the private life, home and correspondence stated in the Constitution of the Republic of Latvia Clause 96. There are also other fundamental rights granted to citizens that could be affected by data retention, such as: freedom of expression, which includes the right to freely receive, keep and distribute information and to express his or her views; freedom of thought, conscience and religion; rights to choose their employment and workplace according to their abilities and qualifications; rights to protection of human honor and dignity. Mentioned fundamental rights result from the Constitution of the Republic of Latvia and also from other legal acts (Civil Law, Law On the Press and Other Mass Media, etc.)

In accordance with the Constitution the state has the obligation to protect fundamental human rights. If they are infringed the aggrieved party has the rights to apply to the court and receive the compensation. If a person considers that their fundamental rights as defined in the Constitution infringe upon legal norms that do not comply with the norms of a higher legal force, the person has the rights to

---

7 www.eps.gov.lv/files/IUMEPLZin_240209_aprite.doc

8 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).

submit a constitutional complaint to the Constitutional Court. A constitutional complaint may be submitted only if all the options have been used to protect the specified rights with general remedies for protection of rights (a complaint to the higher authority or higher official, a complaint or statement of claim to a general jurisdiction court, etc.), except if such do not exist, or if adjudication of a constitutional complaint is of a general interest or if protection of rights with general remedies cannot avert substantial harm for the applicant.

In accordance with the national laws the telecommunications content are the content of the conversations and/or information transferred using the electronic communications network. In accordance with the Criminal Procedure Law the control of telephones and other means of communications without the knowledge of the members of a conversation or the sender and recipient of information could be performed only based on a decision of an investigating judge, if there are grounds for believing that the conversation or transferred information may contain information regarding facts included in circumstances to be proven, and if the acquisition of necessary information is not possible without such operation. In accordance of the Investigatory Operations Law investigatory covert monitoring of non-public conversations (including by telephone, by electronic or other means of communication) and investigatory entry could be performed only in accordance with the special method and with the approval of the Chief Justice of the Supreme Court or a Justice of the Supreme Court specially authorized by him or her.

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

In accordance with the Constitution the mentioned fundamental rights can be restricted if the restriction is determined by law in order to protect the rights of other people, the democratic structure of the State, and public safety, welfare and morals. In accordance with the practice of the Constitutional Court the fundamental rights may be restricted if the restriction is stated in the laws, the restriction correspond to legitimate aim, which the State wants to achieve by setting the restriction and the restriction should comply with the principle of the proportionality, to ascertain whether the public benefit is greater than the loss of the rights and lawful interests of an individual.

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?

Not ruled.

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?

The assessment/balance shall be carried out in each individual case. With respect to data retention in accordance with the Regulations of the Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" authorized institutions, the Office of the Prosecutor and court has to ensure evaluation of the necessity and proportionality of the requests for data retained.

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, the exceptions from the obligation to retain or transmit data are determined in the Criminal Procedure Law and in Investigatory Operations Law.

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 Constitution of the Republic of Latvia Clause 105 defines that „everyone has the right to own property. Property shall not be used contrary to the interests of the public. Property rights may be restricted only in accordance with law. Expropriation of property for public purposes shall be allowed only in exceptional cases on the basis of a specific law and in return for fair compensation". The electronic communications merchants have to ensure and maintain the technical equipment in order to ensure the data retention and transmission to respective institutions for the purposes to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings. Protection of State and public security or investigation of criminal offences, criminal prosecution and criminal court proceedings are the functions of the state institutions, which should be financed by state. In accordance with the Constitution it is not permitted to establish a duty to ensure and maintain the technical equipment which is not necessary in the economic activity of the electronic communications merchants but in order to fulfill the state functions. In my opinion the State is using the equipment of the private parties in order to perform its functions and thereby

restricting the property rights of the electronic communications merchants as far as the equipment used by State are not necessary in the economic activity of the electronic communications merchants. Therefore, in accordance with the Constitution electronic communications merchants have the rights to receive the compensation for the restriction of their property rights.

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)?

With respect to data retention and transmission to entitled authorities, the national law does not determine any conditions or limitations to involve the private actors, except the obligation to pay the compensation for the restriction of the property rights (see question 55).

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

No, except the compensation for the restriction of the property rights (see question 55).

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 stands between Constitution of the Republic of Latvia and the laws. The Administrative Procedure Law states that the legal norms of international law regardless of their source shall be applied in accordance with their place in the hierarchy of legal force of external regulatory enactments. If a conflict between a legal norm of international law and a norm of Latvian law of the same legal force is determined, the legal norm of international law shall be applied.

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 ensure correct transposition of directives into the national law, it is necessary to take the following steps:

1) to clarify the objective and content of the directive;

2) to evaluate the existing national legislative, clarifying whether the national legal acts correspond to the requirements of the directive or whether in the process of

transposition of the directive will be necessary to adopt new legal acts or to amend existing laws;

3) to choose the method for transposing the directive into the national legal acts by evaluating the legal norms of the directive and the legal language and technique of the national law. There are two transposition methods: 1) when the EU legal norms are incorporated into national legal system by rewriting the text of the directive or including the reference into national law to the relevant EU legislation; 2) reformulation method is applied when the objective of the directive is incorporated into the national legal system, not by rewriting the text but by taking over the main point of the legal norms. Depending on the specific matter regulated in the directive, provisions of a directive may be necessary to transpose into the laws, regulations of the Cabinet of the Ministers and in specific cases into the Constitution.

In accordance with the principle of the EU law supremacy, directive is superior to any national law; consequently there are no situations/configurations that might concede to directives a particular status within the hierarchy of norms. Except, in case when directive is not in compliance with the principle of democratic state and the principle of sovereignty of the people of Latvia as stated in the Constitution of the Republic of Latvia. In accordance with the EU principle of direct effect the court is obligated to apply EU law directly if the directive is not implemented into national law, is not implemented correctly or is implemented incompletely.

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 Constitutional court of the Republic of Latvia has stated that the transfer of the competence to EU and implementation of the EU legal norms in the national legal system are acceptable only if EU law is compatible with the principle of democratic state and the principle of sovereignty of the people of Latvia as stated in the Constitution of the Republic of Latvia.

The Constitutional court of the Republic of Latvia has stated that the transfer of competences can not extend so far that it would infringe the grounds of independent, sovereign and democratic republic based on a rule of law and fundamental rights.[9] Therefore, most likely taking into account that the observance of the fundamental rights is a part of the principle of democratic state, transfer of competence also includes a check that the fundamental rights stated in the Constitution are safeguarded in EU level.

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

[9] http://www.likumi.lv/doc.php?id=190439.

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 Data State Inspectorate is the institution which performs the supervision over the data protection in the electronic communications and the Electronic Communications Office creates and maintains the location information data base. The Data State Inspectorate is also the institution which monitors the implementation of the laws on data retention, including application of the procedures stated in the laws for data exchange and watching if the service providers observe technical and organisational requirements with regard to data retention and transfer.

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

In accordance with the Personal Data Protection Law Personal data may be transferred to another state which is not EU or EEA states, if that state ensures such level of data protection as corresponds to the relevant level of the data protection in effect in Latvia, except if the system administrator undertakes to perform supervision regarding the performance of the relevant protection measures. In accordance with the law there is no need to conclude the agreement for transmission of the personal data to other countries which are not EU or EEA states within the sphere of international cooperation, national security and in criminal matters When transmitting the personal data to another country or international organizations it should be notified about all restrictions with respect to the personal data processing. It means that if the retained data are transferred to the third country in the matters of international cooperation, national security and criminal matters the Personal Data Protection Law does not require previous control regarding the data protection in the third country. The institution which transfers the data has an obligation to notify the recipient country regarding the conditions and restrictions for data procession.

IV. Assessment of the overall situation

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

In accordance with the Constitution the rights to inviolability of the private life and correspondence are not absolute and can be restricted in circumstances provided for by law in order to protect the rights of other people, the democratic structure of the State, and public safety, welfare and morals. In accordance with the practice of the Constitutional Court the fundamental rights may be restricted if the restriction is stated in the laws, the restriction correspond to legitimate aim, which the State wants to achieve by setting the restriction and the restriction should comply with the principle of the proportionality. In existing national law the data retention and transmission is performed for investigating the criminal offences, that is, crimes and criminal violence. In my opinion, in order to ensure the principle of proportionality

only crimes may be the occasion for retention the data, therefore it is necessary to ensure that the retained data are used only in cases when investigating the crimes.

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

Latvia

LL.M. Aldis Kalinks

Part 2: Overarching issues and country-specific questions

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

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

There is no general right to communicate anonymously defined in the Constitution of the Republic of Latvia, but the rights to anonymity could be derived from other fundamental rights established in the Constitution, such as the rights to private life, rights to inviolability of correspondence and freedom of speech. For example, in accordance with the Clause 22 of the law On the Press and Other Mass Media, if a person who has provided the information requests that his name is not to be indicated in a mass medium, this request shall be binding. As well as, for example, in accordance with the Clause 14 of the Copyright Law the author of a work have the inalienable moral rights of an author to use anonymity.

The Clause 144 of the Criminal Law establishes the liability of the person who has violated the confidentiality of personal correspondence, information transmitted over a telecommunications network, as well as confidentiality of information and programs provided for use in connection with electronic data processing.

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

There have been drafted new amendments to the Electronic Communications Law with regard to data retention which are submitted to the Saeima (Parliament) of the Republic of Latvia now and accepted in the first reading (in order to adopt amendments to laws usually there are three readings)1.

The draft amendments to the Electronic Communications Law establish new obligations of the electronic communications merchants with regard to personal data protection. The draft amendments define that in addition to the rules of the Personal Data Protection Law, electronic communications merchants shall have to 1) ensure that only authorized persons can access the personal data and that the data are used only for the purposes stated in this law; 2) ensure that personal data are protected from unlawful or unintentional destruction or unintentional loss and from unlawful and unintentional procession, preservation, access or exposure; 3) document the internal procedure for examination and prevention of the breach of personal data protection. It is also planned to adopt the regulations of the Cabinet of Ministers which are going to establish requirements that electronic communications merchants will have to observe when drafting the internal procedure for examination and prevention of the breach of personal data protection.

In accordance with the draft amendments, the Electronic Communications Law is going to establish the obligation of the electronic communications merchants to inform the Data State Inspectorate about any breach of personal data protection as well as to inform the subscriber, user or data subject of the breach of personal data protection in case the infringement can cause consequences to mentioned persons or to their privacy. Electronic communications merchants will have an obligation to retain information about the breach of personal data protection for 18 months.

The draft amendments define the obligation of the electronic communications merchants to transfer retained data also to the Competition Council of the Republic of Latvia for the purposes of investigating the breaches of the competition rights in the sphere of prohibited agreements.

The draft amendments establish the obligation of the electronic communications merchants to provide retained data to the courts in the civil cases. Electronic communications merchants will have an obligation 1) subject to request of the court

[1] http://titania.saeima.lv/LIVS10/SaeimaLIVS10.nsf/0/9B12FE972AB318C5C22578810021553E?OpenDocument.

to provide the information about name, surname or title and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the connection, in order to protect the infringed rights and legal interests of the person in the electronic environment within the civil cases; 2) subject to the request of the court to provide also information about traffic data which are substantial in the examination of the case and which exposure the court has recognized as possible by balancing the exposure of retained data with the persons rights to the personal data protection. The draft amendments to the Electronic Communications Law provide the rights to the electronic communications merchants to request from the applicants to compensate expenses which have occurred when providing the required information.

The different arguments uttered by the Ministry of Justice of the Republic of Latvia when deciding on necessity to amend the Electronic Communications Law was conflict between data retention and rights to personal data protection and inviolability of correspondence. In the Report of the Ministry of Justice "The proposed changes in regulations in order to enable a person to defend their rights in court in case of civil infringement on the internet, and the opportunity to receive adequate legal protection"2the ministry has indicated that the exposure of the retained data without the consent of the data subject substantially infringes the fundamental rights of the person. On the other hand, it is recognized that if the courts do not have rights to request these data there will be no other possibility to clarify the defendant within the civil proceedings in the cases when the rights to honour and dignity is infringed in the internet.

There are no publicly available discussions about my proposals for improvements mentioned in my answer to question 63 of the first questionnaire. As well as, there are no publicly available discussions regarding "quick freeze" option as potential alternative to data retention. The "quick-freeze" effect is already foreseen in the Clause 191 of the Criminal Procedure Law, which states that "(1) A person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system. (2) The duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days". This regulation is additional to the data retention obligation as stated in the Clause 192 of the Criminal Procedure Law.

It is also planned to provide similar regulation applicable in the civil cases.

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-**

[2] www.mk.gov.lv/doc/2005/TMZino_140211_GrESL.140.docx.

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?

In accordance with the Clause 191 of the Criminal Procedure Law (please see my answer to question 2) the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) pursuant to the decision of a person directing the proceedings have also an obligation to store specific data, the retention of which is not specified by law.

In accordance with the law On the Prevention of Money Laundering and Terrorism Financing the subjects determined in this law such as credit institutions, financial institutions, tax advisors, external accountants, sworn auditors and commercial companies of sworn auditors, sworn notaries, sworn lawyers, other independent providers of legal services etc. have an obligation to perform client identification and in cases specified in the law also client due diligence in order to prevent money laundering and terrorism financing. The mentioned subjects have an obligation to notify the office for Prevention of Laundering of Proceeds Derived from Criminal Activity regarding each unusual or suspicious transaction. The report to be submitted to the office for Prevention of Laundering of Proceeds Derived from Criminal Activity should comprise the following information: 1) the customer identification data; 2) a description of the planned, proposed, consulted, commenced, deferred, executed or approved transaction, as well as the identification data of the person participating in the transaction and the amount of the transaction, the time and place of the transaction executed or proposed and, if there are documents attesting to the transaction at the disposal of the subject of the law, the copies of such documents; and 3) the basis on which the subject of the law considers the transaction to be suspicious, or the unusual transaction indication to which the relevant transaction conforms. The subjects of the law who have reporting obligation have an obligation to store the following documents at least for five years after the end of business relationships: 1) copies of the documents attesting to the customer identification data; 2) information on the customer and the accounts thereof; 3) the notification regarding the beneficial owner; 4) correspondence, including electronic mail correspondence; and 5) other documents, including electronic documents obtained in the process of customer due diligence. In special cases, the time period may be extended, upon the instructions of the office for Prevention of Laundering of Proceeds Derived from Criminal Activity, but it shall not exceed six years.

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?

In accordance with the Clause 110 Paragraph 2 Section 2 and Clause 98 Paragraph 2 of the Criminal Procedure Law a witness and victim in the criminal proceedings has the right to refuse to testify against him/her. The Clause 63, Clause 66, Clause 70 and Clause 503 of the Criminal Procedure Law establishes the right of suspect, detained person and accused to refuse to provide testimony. In accordance with the Clause 10 of the Criminal Procedure Law also person who has immunity from criminal proceedings is completely or partially released from participation in criminal proceedings, which inter alia include provision of evidence and the issuance of documents and objects.

The Clause 126 of the Criminal Procedure Law establishes "indirect" obligation of the person who has the right to assistance of a defence counsel to indicate circumstances that exclude his criminal liability, as well as indicate an alibi. In case the person fails to indicate such circumstances or alibi, the prosecution does not have a duty to prove the non-existence thereof. In this case the person will not be able to receive compensation for losses that have occurred when unjustifiably regarding him as a suspect, if the termination of criminal proceedings or the acquittal of the person is related to the ascertaining of the referred to circumstances.

The principle of fair court established in the Clause 92 of the Constitution of the Republic of Latvia as well as in the Clause 6 of the European Convention on Human Rights comprises the privilege against self-incrimination which is made up from the right of silence and not to be compelled to produce inculpating evidence. Therefore, in my opinion, taking into account the self-incriminating privilege, the accused person do not have an obligation to collect evidence, such as data retained, that incriminate him/her and transmit them to investigative authorities. The privilege against self-incrimination does not prohibit the entitled bodies to request the retained data from the electronic communications merchants. In accordance with the Paragraph 1 of the Clause 190 of the Criminal Procedure Law a person directing the proceedings is entitled to request from natural or legal persons objects, documents and information regarding the facts that are significant to criminal proceedings.

The conflict between data retention obligation and rights to refuse to testify may arise in cases when the electronic communications merchant is the person in criminal proceeding who has the rights not to testify against it. In this case it should be observed that the obligation of the electronic communications merchants to retain and transmit data is established with the Electronic Communications Law, which could be considered as special law against Criminal Procedure Law. Therefore, in my opinion, the rights of the electronic communications merchants established in the Criminal Procedure Law not to testify and collect evidence against it could be restricted.

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

   The retained data obtained by entitled bodies are added to the criminal case materials and after examination of the case stored in the archives of respective entitled bodies.

   In accordance with the Cabinet of Ministers Regulations No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" authorized institutions, the Office of the Prosecutor and court must ensure protection of the received data to be retained in accordance with the regulatory enactments which regulate information protection. Therefore, entitled bodies must observe the measures prescribed in the Personal Data Protection Law and the Regulations of the Cabinet of the Ministers No. 40 "The compulsory technical and organizational requirements for protection of personal data" (please see my answer to the question 40 in the first questionnaire). Protection of criminal materials is also defined in the Criminal Procedure Law. In accordance with the Clause 375 of the law the materials located in the criminal case are a secret of the investigation, and only officials who perform the criminal proceedings, as well as the persons to whom they have rights to present the relevant materials in accordance with the procedures provided in the law, are permitted to be acquainted with such materials.

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.**

   In the Public Report of the Data State Inspectorate for year 2009, was indicated that "In year 2009 the Data State Inspectorate summarized the statistical data about requests of the retained data and transmission of these data. The statistical data were submitted by 88 merchants in total for 26 096 requests. In accordance with the Clause 10 of the Directive 2006/24/EC prepared information was sent to the European Commission"3. There is no other publicly available information regarding statistical data of the requests.

---

[3] http://www.dvi.gov.lv/par_mums/dvi_parskats_2009.pdf .

B. Country-specific questions

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

The Clause 96 of the Constitution of the Republic of Latvia states that "Everyone has the right to inviolability of his or her private life, home and correspondence". The rights to inviolability of correspondence and rights to private life established by the Constitution are not absolute and can be restricted in accordance with the Clause 116 of the Constitution, which declares that "The rights of persons set out in Articles ninety-six, […] of the Constitution may be subject to restrictions in circumstances provided for by law in order to protect the rights of other people, the democratic structure of the State, and public safety, welfare and morals. […]".

Therefore, the rights to inviolability of correspondence and rights to private life can be restricted if 1) restriction is stated in the law; 2) restriction corresponds to legitimate aim and 3) restriction is necessary in the democratic society.

The rights to retain and transfer data are established in the Electronic Communications Law and in the Regulations of the Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" as well as the protection of data retained are also regulated by the legislation acts such as the Personal Data Protection Law and Regulations of the Cabinet of Ministers No. 40 "The compulsory technical and organizational requirements for protection of personal data", which explicitly define the procedure of retention, transfer and protection of data retained.

The aim of the data retention and transmission and therefore also for restriction of the rights to private life and inviolability of correspondence is stated in the Clause 71 1of the Electronic Communications Law, which defines that "Data to be retained shall be retained and transferred […] in order to protect State and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings". Therefore, restrictions of the rights to private life and inviolability of the correspondence are established to protect the public safety which in accordance with the Clause 116 of the Constitution is considered to be legitimate aim.

In order to evaluate whether these restrictions are necessary in the democratic society, it is necessary to evaluate if these restrictions are socially needed and proportionate. It could be considered that transfer of retained data for the purposes stated in the Clause 711 of the Electronic Communications Law is socially needed in order to protect the public safety. The proportionality principle requires to ensure the balance between restrictions of the rights of a person and benefit of all society.

Taking into account that these restrictions are applied in order to ensure the public safety, in my opinion, there can be no doubts that the benefit gained by society is greater than the violation of the person's rights to inviolability of correspondence and private life.

In order to recognize that the proportionality principle is observed it is also necessary to evaluate whether the legitimate aim cannot be reached by other less restrictive means. In my opinion other means such as "quick-freeze" option will not effectively ensure the attainment of legitimate aim due to the fact that "quick-freeze" option could be used only when the crime has already been detected or a potential perpetrator of a crime identified.

As I have already indicated in the first questionnaire in order to improve the data retention regime it would be necessary to ensure that the retained data are used only in cases when investigating the crimes not all criminal offences as it is stated in the present wording of the Electronic Communications Law. In my opinion, the draft amendments to the Electronic Communications Law as described in my answer to question No.2, which are going to establish the obligation of the electronic communications merchants to transfer retained data also in the civil cases, are not in compliance with the proportionality principle that must be observed when restricting the fundamental rights.

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

The Clause 96 of the Constitution of the Republic of Latvia states that „Everyone has the right to inviolability of his or her private life, home and correspondence".

In accordance with the decision of the ECHR in case Malone v. The United Kingdom4, the court has recognized that also administrative data concerning telephone calls are integral element in the communications made by telephone and release of such information without the consent of the subscriber also amounts to an interference with a right guaranteed by Article 8 of European Convention on Human Rights.

Taking into account that in accordance with the decisions of the Constitutional Court of the Republic of Latvia the case law of the ECHR is mandatory with regard to interpretation of the legal norms of the European Convention on Human Rights and conclusions of the ECHR are also applicable to the interpretation of the Clauses of the Constitution of the Republic of Latvia, therefore, in my opinion, the data retained in accordance with the Directive and Electronic Communications Law are covered by the inviolability of correspondence. This conclusion is also expressed by the Ombudsman of the Republic of Latvia5.

---

4 Malone v. The United Kingdom, judgment of 2 August 1984.

5 http://www.tiesibsargs.lv/lat/petijumi_un_viedokli/viedokli/?doc=199.

9. **Does your answer to question 58 of the first questionnaire mean that while the *ECHR* stands between the Constitution and other Latvian law, international law *generally* has the same rank as ordinary national (Latvian) law? Is international law *directly* applicable in Latvia without the need to transpose it into national law?**

In accordance with the Paragraph 3 of the Clause 15 of the Administrative Procedure Law if a conflict between a legal norm of international law and a norm of Latvian law of the same legal force is determined, the legal norm of international law shall be applied. In accordance with the Clause 16 of the Constitutional Court Law the Constitutional Court shall adjudicate matters regarding: 1) compliance of laws with the Constitution; 2) compliance of international agreements signed or entered into by Latvia (also until the confirmation of the relevant agreements in the Saeima) with the Constitution; 3) compliance of other regulatory enactments or parts thereof with the norms (acts) of a higher legal force; 4) compliance of other acts of the Saeima, the Cabinet, the President, the Speaker of the Saeima and the Prime Minster, except for administrative acts, with law; 5) compliance with law of such an order with which a Minister authorized by the Cabinet has suspended a decision taken by a local government council (parish council); and, 6) compliance of Latvian national legal norms with those international agreements entered into by Latvia that is not in conflict with the Constitution. The Paragraph 4 of the Clause 32 of the Constitutional Court Law states that if the Constitutional Court has declared any international agreement signed or entered into by Latvia as non-compliant with the Constitution, the Cabinet of the Ministers has the duty to provide for amendments to this agreement without delay, the denunciation of this agreement, the suspension of its operation or the revocation of accession.

Therefore, the international law has a higher rank than national law but the international law must be in conformity with the Constitution of the Republic of Latvia.

In accordance with the Paragraph 1 of the Clause 68 of the Constitution of the Republic of Latvia "All international agreements, which settle matters that may be decided by the legislative process, shall require ratification by the Saeima". The international agreements are ratified by the legislator with the national law. Despite the fact that international agreements are ratified with the national laws, the opinion of the legal experts in Latvia is that the international agreements are applicable directly because after ratification the international agreements do not change its international nature.6 Also the Constitutional Court of the Republic of Latvia in its decision refers directly to the international law and not to national law in accordance to which the agreement is ratified.7

10. **Is the constitutionally fixed limit to a conferral of national sovereignties to the EU (see your answer to question 60 of the first questionnaire) in any way binding for representatives of your country in EU organs and institutions (e.g.**

---

6 http://www.juristavards.lv/index.php?menu=DOC&id=224675.

7 http://www.likumi.lv/doc.php?id=153590.

the Council of Ministers, the European Council) when exercising their functions in the adoption and execution of an EU legislative act?

In my opinion, taking into account that these representatives represent the interests of Latvia in European Union organs and institutions, the restrictions to transfer the national sovereignties to the EU mentioned in my answer to question 60 are binding to them. These representatives may not act against the Constitution of the Republic of Latvia.

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

    There are no rules preventing the same data from being retained more than once. The national rules do not clearly establish who are responsible to retain data for the purposes mentioned in the Directive in case when the network operator and the service provider are different legal personalities. From unofficial information it is being known that in practice there are cases when service provider and network operator conclude an agreement which regulates the obligations of the network operator to retain data, in this way avoiding to retain data more than once time.

12. **An English translation of the Cabinet of Ministers Regulations No. 40 of 2001 can be found at: http://www.dvi.gov.lv/eng/legislation/requirements/. However, it seems to be outdated, as the Latvian page shows a newer version with latest changes made in 2007. Could you please specify which changes have been made to the 2001 version of the text (own translation of the relevant passages)? Please also specify where in the Regulations the rules set out in your answer to question 40 of the first questionnaire are laid down.**

    The amendments to the Regulations of the Cabinet of the Ministers No. 40 "The compulsory technical and organizational requirements for protection of personal data" have been made taking into account the amendments to the Personal Data Protection Law. In accordance with the amendments to these regulations the following changes have been made on August 28, 2007:

    1) Amendments to the title of these regulations. Previous title was "Obligatory technical and organizational requirements for protection of personal data processing systems". In accordance with the amendments, the title of the regulations in present wording is the following "The compulsory technical and organizational requirements for protection of personal data". In accordance with the amendments, the words "processing systems" are deleted not only from the title but also from all text of these regulations. These changes have been made because the technical and organizational requirements must be applied not only to the personal data that are incorporated in the processing systems but to personal data in general;

    2) Amendments to the reference that specifies the law and clause in accordance to which the regulations are issued. In accordance with the previous wording the

reference stated that the regulations are issued in accordance with the Clause 26 of the Personal Data Protection Law. In accordance with the new wording, the reference states that the regulations are issued in accordance with the Paragraph 1 of the Clause 26 of the Personal Data Protection Law;

3) The Section 1 of the regulations is expresses in the following wording:

"These regulations define obligatory technical and organizational requirements for protection of personal data which must be taken into account when processing personal data.";

4) The Section 3 and Section 3.1. of the regulations are expressed in the following wording:

"3. Obligatory technical protection of personal data is carried out with physical and logical protection means providing: 3.1. protection against threats to personal data caused by physical impacts.";

5) The Section 4. and Section 4.4. of the regulations are expressed in the following wording:

"4. When carrying out personal data processing, administrator shall provide that: 4.4. transfer of technical resources which are used to process personal data is carried out only by exclusively authorized person.";

6) The Sections 4.6.,4.6.1., 4.6.2., 4.6.3., 4.6.4. of the regulations are expressed in the following wording:

"4.6. When receiving personal data, information should be retained on: 4.6.1. time when personal data are received; 4.6.2. person who has delivered personal data; 4.6.3. person who has received personal data; 4.6.4. personal data which are received.";

7) The Section 5 and Section 5.1. of the regulations are expressed in the following wording:

"5. System administrator, when processing personal data, elaborates internal data processing protection provisions, where are established: 5.1. responsible persons for information resources, technical resources and protection of personal data, their rights and obligations.";

8) The regulations are supplemented with the Section 5.11. in the following wording:

"5.11. rights, obligations, restrictions and liability of the persons who use the personal data.";

9) The Section 6 of the regulations is expressed in the following wording:

"6. System administrator each year carries out interior audit of personal data processing and prepares overview of activities, which were performed in sphere of information protection.";

10) The Section 7 of the regulations is expresses in the following wording:

"7. System administrator informs persons, which process the personal data on compulsory technical and organizational requirements for protection of personal data.";

The rules set out in answer to question 40 a) are stated in the Section 5 of the regulations. The rules set out in answer to question 40 b) are stated in the Section 4 of the regulations. The rules set out in answer to question 40 c) are stated in the Section 5.11. of the regulations. The rules set out in answer to question 40 d) are stated in the Section 4 and Section 5 of the regulations. The rules set out in answer to question 40 e) are stated in the following Sections 5.1., 5.4., 5.7. and the rules set out in answer to question 40 g) are stated in the Section 5.4. and Section 5.11.of the regulations.

No. 2 of the Regulations previously referred to the Regulations No. 106 of the Cabinet of Ministers "Security regulations for information systems", whereas this reference seems to have been repealed in the latest version. Can you explain why this has happened?

Section 2 of the regulations was excluded because the Regulations No. 106 of the Cabinet of Ministers "Security regulations for information systems" became invalid in December 5, 2002.

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 regulations and the Paragraph 1 of the Clause 26 of the Personal Data Protection Law in accordance to which these regulations are issued do not specify that these regulations apply only to the data retention, therefore it is considered that the regulations apply to any data processing.

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

The State Administration Structure Law establishes general rules on co-operation in state administration. The Clause 54 of the State Administration Structure Law

defines that institutions co-operate in order to perform their functions and tasks. Institutions may co-operate both in individual cases and continuously. When co-operating continuously, institutions may enter into interdepartmental agreements. Institutions may enter into interdepartmental agreements also if they belong either to one public person or to various public persons. The competence of institutions prescribed by regulatory enactments may not be delegated or altered by an interdepartmental agreement.

Institutional co-operation shall be free of charge, unless prescribed otherwise in external regulatory enactments. In accordance with the Clause 55 of the State Administration Structure Law institutions can co-operate in the following matters: 1) an institution may propose that another institution ensure the participation of individual administrative officials in the performance of particular administrative tasks; 2) an institution, observing the restrictions prescribed by regulatory enactments, may propose that another institution provide the information that is at its disposal; 3) an institution may propose that another institution provide it with an opinion on a matter that is in the competence of the institution that provides the opinion. Institutions within their competence may agree also on other co-operation subject-matter.

An institution may refuse to co-operate, by substantiating the refusal in writing, if: 1) co-operation is impossible due to practical reasons; 2) co-operation is impossible due to legal reasons; 3) another institution may be involved in the co-operation with less expenditure of resources; or 4) the necessary expenditure of resources exceeds the necessity of the institution that proposed the co-operation for such co-operation. An institution that has received a refusal to co-operate, may invite a higher institution of the institution that has given the refusal to evaluate the justification for such refusal.

More specific rules of co-operation are determined in laws which inter alia regulate the obligations and rights of respective institutions. For example, the Clause 394 of the Criminal Procedure Law states that an institution may assign the performance of separate procedural actions or tasks to another investigating institution or to official authorized to perform criminal proceedings. In accordance with the Clause 19 of the Law on State Security Institutions state security institutions have the rights within their competence to receive necessary information, documents and other materials from the state and municipal institutions and officials; to become acquainted and to have access to the information mediums, materials of the archive and other documents of the state and municipal institutions.

The Clause 396 of the Criminal Procedure Law stipulates that the information acquired in the pre-trial criminal proceedings until the completion thereof shall be divulged only with the permission of an investigator or a public prosecutor and in the amount specified by him or her. In accordance with the Clause 375 of the Criminal Procedure Law during criminal proceedings, the materials located in the criminal case shall be a secret of the investigation, and only the officials who perform the criminal proceedings, as well as the persons to whom the referred have

the rights to present relevant materials in accordance with the procedures provided for in this law, are permitted to get acquainted with such materials.

Taking into account that the Clause 71 [1] of the Electronic Communications Law and Regulations of Cabinet of Ministers No. 820 "Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled" explicitly define the authorities and purposes in accordance to which the retained data can be transferred and taking into account the rules of Criminal Procedure Law regarding protection of the criminal case materials, therefore it could be considered that the entitled bodies have no rights to transfer retained data to other authorities for purposes other than stated in the Electronic Communications Law.

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

In accordance with the Clause 2 of the Office of the Prosecutor Law the Office of the Prosecutor supervises the investigative activities and investigatory operations, intelligence or counterintelligence process of the state security institutions. The Office of the Prosecutor is independent institution in the sense of what have been said in question 35 of the first questionnaire.

With regard to supervising the Office of the Prosecutor, in accordance with the Clause 41.[3] Paragraph 2 of the Office of the Prosecutor Law the Saeima of the Republic of Latvia at the request of one third of its members and the Chief Justice of the Supreme Court can propose an investigation to determine whether the Prosecutor General has acted in accordance with the law. The investigation is performed by a justice of the Supreme Court specially authorized by the Chief Justice, which is independent authority in the sense of what have been said in question 35 of the first questionnaire.

With regard to supervising the courts, in accordance with the Clause 3 of the Judicial Disciplinary Liability Law the following are entitled to initiate a disciplinary matter against judges: 1) the Chief Justice of the Supreme Court – regarding judges of district (city) courts, regional courts judges and senators (judges of the Senate) of the Supreme Court, 2) the Minister for Justice – regarding judges of district (city) courts and regional courts, 3) the Chief Judges of regional courts – regarding judges of district (city) courts and regional courts judges, 4) the Chief Judges of district (city) courts – regarding judges of district (city). All mentioned persons and institutions are independent in the sense of what have been said in question 35 of the first questionnaire.

15. **Your answer to question 45 of the questionnaire refers to the discussions between public bodies regarding the data retention regime. Has there also been a debate in civil society (e.g. among civil rights groups, the affected business sectors etc) about the concept of data retention? If so: please describe the main positions that have been expressed in this debate.**

    There are no other publicly available debates regarding data retention regime.

Brief update on the situation in Latvia on data retention (August 2013)

After finalizing the report on INVODAS project on data retention in year 2011, there has been made some amendments to the legal acts regulating the data retention in Latvia.

Please see below the main amendments to the Electronic Communications Law with respect to the data retention:

In accordance with the Electronic Communications Law it is now established that retained data can be used not only in criminal cases but also in the civil cases. In accordance with the Clause $71.^2$ Part 1 and Part 2 of the Electronic Communications Law **(**The Electronic Communications Law with the last amendments made on 8 June 2011 is available at: *http://www.vvc.gov.lv/advantagecms/LV/meklet/meklet_dokumentus.html?query=Electronic%20Communications%20Law%20&resultsPerPage=10*) it is stated that in order to ensure the protection of the rights and legal interests of the individual infringed in the electronic environment in the civil cases an electronic communications merchant has an obligation, upon the request of the court, to ensure the provision of the information regarding the given name, surname or title and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the connection.

In order to ensure the before mentioned rights and legal interests of the individual the electronic communications merchant upon the request of the court has an obligation to ensure the provision of the information also regarding traffic data having the importance in the case, disclosure of which has been recognised as permissible by the court in the case weighing it against the right of the individual to data protection thereof.

The Electronic Communications Law also establishes new obligations of the electronic communications merchant with respect to data protection (such as to ensure that personal data can be accessed only by authorised personnel and used for previously specified purposes, protected against accidental or unlawful destruction or accidental loss, and unauthorised or unlawful storage, processing, access or disclosure etc.), as well as the law establishes the obligation to the electronic communications merchant to inform the State Data Inspectorate, as well as the data subject of a breach of personal data protection (please see Clause 68^1, Clause 68^2, Clause 68^3 and Clause 68^4 of the Electronic Communications Law).