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

Estonia

Pirkko-Liis Harkmaa, LAWIN

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

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

I. Legal provisions

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

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

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

The Directive has been transposed into Estonian law with the Act Amending Electronic Communications Act and Public Health Act, which was adopted on 15 November 2007. Technically, this act introduced amendments into Electronic Communications Act (ECA). Hence, we have hereinafter referred to the relevant provisions of ECA.

- ***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)?**

   N/A

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?**

   N/A

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.**

   N/A

- ***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 Act Amending Electronic Communications Act and Public Health Act is not available in English. An unofficial translation of the ECA, which contains also the amendments introduced by that act (the most important provision for the transposition of the directive is § 1111), is available here: http://www.tja.ee/public/documents/Elektrooniline_side/Oigusaktid/ENG/Electronic_Communications_Act.pdf

   It should be noted that the English translation does not contain the latest amendments to the ECA. However, such later amendments do not concern data retention.

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

   As noted under Question 1, the Act Amending Electronic Communications Act and Publish Health Act, which transposed the Directive, was adopted on 15 November 2007. The provisions regarding data retention entered into force in two phases – most of the relevant provisions entered into force on 1 January 2008, but the obligations of providers of Internet access, Internet e-mail and Internet telephony services, set out in § 1111(3) of the ECA, entered into force on 14 March 2009. This

was in accordance with the Estonia's declaration pursuant to Article 15(3) of the Directive, whereby Estonia postponed the application of the Directive to retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption of the Directive.

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 Directive was transposed by an Act of Parliament, which introduced amendments into an earlier Act of Parliament, namely the ECA. The amendment incorporated into the ECA the most important aspects of the Directive (e.g. provisions about an obligation to retain data, types of data to be retained, data protection and safety etc.). Some more technical matters are regulated by the minister's regulation, namely, Regulation No 56 of the Minister of Economic Affairs and Communication of 25 June 2008 "The procedure for retention, passing over to Technical Surveillance Board, deleting and destroying data, inquiries, log files and applications"1. To our opinion the chosen legal acts correspond to those usually chosen in Estonia for such kind of matters.

8. **Are the terms defined in 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 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 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?**

   Unlike the Directive, the ECA does not define the terms "data" (defined in the Art. 2 para. 2(a) of the Directive).

   As regards the term "user" (defined in Art. 2 para. 2(b) of the Directive), the ECA does not contain the exact equivalent, but it nevertheless contains the definitions of the terms "subscriber" and "end user". According to § 2, clause 15 of the ECA, "subscriber" is a person using a publicly available electronic communications

[1] Available: http://www.riigiteataja.ee/ert/act.jsp?id=13100712 (only in Estonian).

service who has a contract with a communications undertaking for the use of the publicly available electronic communications service, and according to § 2, clause 27 of the ECA, "end-user" is a subscriber who does not provide a publicly available electronic communications service. Hence, as apparent for the definitions, the ECA contains definitions of subscribed users only. However, § 1111 of the ECA, which sets out the data retention obligation, refers also to "user".

The term "telephone service" is defined in § 2, clause 58 of the ECA as publicly available electronic communications service for originating and receiving national and international calls at a determined location and for access to emergency services through a number or a short access code connected with the number in the Estonian or international telephone numbering plan. This definition is narrower than the definition is Art. 2 para. 2(c) of the Directive, which includes also supplementary services, messaging and multi-media services.

The term "user ID" is defined in § 2, clause 121 of the ECA as a unique identifier allocated to subscribers for using an Internet access service or Internet communications service. This definition appears similar to the one contained in Art. 2. para 2(d) of the Directive.

The term "cell ID" is defined in § 2, clause 201 of the ECA as the identity of the cell from which a mobile telephone service originated or in which it terminated. This definition is identical to the one in Art. 2 para 2(e) of the Directive.

As regards "unsuccessful call attempts" defined in Art. 2 para. 2(f) of the Directive, the ECA contains two definitions – § 2, clause 42 defines "unsuccessful call" as a case where a call has been successfully connected but not answered or there has been an electronic communications network management intervention, and § 2, clause 181 defines "call attempt" as a case where connection was not established. Hence, for the purposes of the ECA, "unsuccessful calls" mean the same as "unsuccessful call attempts" in the meaning of Art. 2 para. 2(f) of the Directive.

In addition to the foregoing, § 2 of the ECA contains a large list of other definitions (please see the referred English translation of the ECA). Several of these definitions coincide with the definitions set out in Directives 2002/21/EC and 2002/58/EC. The terms defined in Directive 95/46/EC are defined in the Personal Data Protection Act,[2] which was adopted on 15 February 2007 and entered into force on 1 January 2008.

[2] Unofficial English translation of the Personal Data Protection Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=XXXX041&keel=en&pg=1&ptyyp=RT&tyyp=X&query=isikuandmete.

Dimension 1 (State - citizen)

9. What data have to be retained according to the national rules transposing the Directive? Do these rules include additional retention obligations with regard to traffic data that go beyond the obligations mentioned in the Directive (e.g. location data resulting from the use of mobile email services), or do national retention obligations fall short of those specified by the Directive? Do data on unsuccessful call attempts have to be retained?

The retention obligations are mainly set out in the §§ 1111(1)-(3) of the ECA[3]. In summary, the referred provisions of the ECA broadly follow the obligations set out

[3] § 111[1]. Obligation to retain data

(1) Communications undertakings shall retain data that are necessary for the performance of the following acts:

1) tracing and identification of the source of a communication;

2) identification of the destination of a communication;

3) identification of the date, time and duration of a communication;

4) identification of the type of communications service;

5) identification of users' terminal equipment or what purports to be their terminal equipment;

6) identification of the location of terminal equipment.

(2) Telephone or mobile telephone service providers and telephone network and mobile telephone network service providers shall retain the following data:

1) the telephone number of the calling party and the name and address of the subscriber;

2) the telephone number of the called party and the name and address of the subscriber;

3) the number dialled and the name and address of the subscriber in cases involving supplementary services, including call routing or call transfer;

4) the date and time of the start and end of the call;

5) the telephone or mobile telephone service used;

6) the International Mobile Subscriber Identity (IMSI) of the calling party and the called party;

7) the International Mobile Equipment Identity (IMEI) of the calling party and the called party;

8) the cell ID at the time of commencement of the call;

9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are retained;

10) in the case of pre-paid anonymous mobile telephone services, the date and time of the initial activation of the service and the cell ID from which the service was activated.

(3) Providers of Internet access, Internet e-mail and Internet telephony services shall retain the following data:

1) the user IDs allocated by a communications undertaking;

2) the user ID and telephone number allocated to any communication entering the telephone network or mobile telephone;

in Art.. 5 of the Directive, although with some difference regarding the arrangement of the list of obligations and use of some terms. There are two more substantive differences:

a) § 1111(1) of the ECA sets out general retention obligation, which is not set out in Art. 5 of the Directive. Namely, according to this provision, communications undertakings are to retain data necessary for the performance of the following acts: tracing and identification of the source of a communication; identification of the destination of a communication; identification of the date, time and duration of a communication; identification of the type of communications service; identification of users' terminal equipment or what purports to be their terminal equipment; and identification of the location of terminal equipment. This obligation is only of general nature and is not referred to in other provisions of the ECA, which regulate quality, maintenance, use, etc. of the data to be retained under § 1111(2)-(3) of the ECA.

b) The list of obligations of telephone or mobile telephone service providers (§ 1111(2) of the ECA) does not contain the equivalent to the obligation set out in Art. 5 para 1(e)(1) of the Directive.

As regards unsuccessful call attempts, the ECA follows the Article 3(2) of the Directive. Accordingly, unsuccessful call attempts within the meaning of Art. 2 para. 2(f) of the Directive must be retained, but unconnected calls do not have to be retained (§ 1111(8) of the ECA). [4]

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.

As a general rule, a communications undertaking is required to maintain the confidentiality of all information which becomes known thereto in the process of

---

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

4) the user ID or telephone number of the intended recipient of an Internet telephony call;

5) the name and address of the subscriber and user ID of the intended recipient of the communication in the case of Internet e-mail and Internet telephony services;

6) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, allocated by the Internet access service provider to a user and the user ID;

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

8) the Internet service used in the case of Internet e-mail and Internet telephony services;

9) the calling telephone number in the case of dial-up Internet access;

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

[4] As noted in the answer to question 8 above, the ECA uses the term "unsuccessful call" instead of "unsuccessful call attempts" and it uses the term "call attempt" instead of "unconnected call"

provision of communications services and which concerns subscribers as well as other persons who have not entered into a contract for the provision of communications services but who use communications services with the consent of a subscriber. In particular, the following data must be protected: specific data of using communications services; the content and format of messages transmitted through the communications network; and information concerning the time and manner of transmission of messages (§102(2) of the ECA). Such information may be disclosed only to the relevant subscriber and, with the consent of the subscriber, to third persons.

There are certain clarifications to this rule:

1) Notification of the subscriber – processing of the information obtained through provision of communications services is allowed if the communications undertaking notifies the subscriber, in a clear and unambiguous manner, of the purposes of processing the information, and gives the subscriber an opportunity to refuse the processing (§ 102(3) of the ECA).

2) Business-related recording and exchange of information – a communications undertaking may collect and process, without the consent of a subscriber, information which must be processed for the purposes of recording the transactions carried out in the conduct of business activities and for other business-related exchange of information (§ 102(4) of the ECA).

3) Provision of services – a communications undertaking may store or process data without the consent of a subscriber if the sole purpose of such activity is the provision of services through the communications network, or if such activity is necessary for the provision of the information society services, which are directly requested for by the subscriber (§ 102(4) of the ECA).

4) Marketing purposes – if a communications undertaking wishes to process information for marketing purposes with the subscriber's consent, the undertaking must inform the subscriber, prior to obtaining the consent, of the type of information needed for such purposes and the duration of the intended use of such information. A communications undertaking may use information, which the undertaking is permitted to use for marketing purposes, only until it is necessary for achieving the relevant goal. If the subscriber so desires, the communications undertaking must provide the subscriber with details concerning the use of the information (§ 103 of the ECA).

5) Billing purposes – a communications undertaking may process the information without the subscribers' consent if such activity is necessary for billing the subscribers, including for the determination and calculation of interconnection charges (§ 104 of the ECA).

6) Location data – a communications undertaking may process subscribers' location data, only if such data are rendered anonymous prior to processing (except to the extent necessary for billing purposes or as required under data retention obligation). Nevertheless, upon subscriber's consent, a

communications undertaking may also process location data to provide other services without rendering the data anonymous, but only to an extent and during the term necessary for processing. Before obtaining the consent of a subscriber, a communications undertaking must inform the subscriber of the data needed for the provision of services, the purpose and term of using such data and whether such data are forwarded to third persons for the purposes of providing the services. A subscriber has the right to withdraw the consent at any time. Moreover, a subscriber who has granted consent for the processing of location data must have easy opportunity to temporarily prohibit, free of charge, the processing of the data in the part of establishment of the connection or transmission of the information indicated thereby. (§ 105 of the ECA).

Processing, including retention of electronic communications data, beyond the data to be retained in accordance with the Directive, is also regulated in Personal Data Protection Act. According to §4(1) of the Personal Data Protection Act, personal data are any data concerning an identified natural person or a natural person to be identified, regardless of the form or format in which such data exists. Hence electronic communications are also included.

According to § 10(1) of the Personal Data Protection Act processing of personal data are permitted only with the consent of the data subject unless otherwise provided by law. There are several exceptions, which allow processing of personal data without consent of data subject (§ 14 of the Personal Data Protection Act). Please see more detailed overview of regulation set out in the Personal Data Protection Act under answer to question 26.

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

The national rules transposing the Directive do not contain specific rules on the purposes for which data retention is mandated. It is only possible to conclude on the basis of the rules transposing the Directive that communications undertakings must provide retained data in repose to the queries of the surveillance and security authorities and courts (§§ 112 and 1141 of the ECA).

More specific conditions which may justify such requests can be derived from other legal acts, such as the Code of Criminal Procedure[5], Surveillance Act[6], Security Authorities Act[7], Code of Civil Procedure[8] and Securities Market Act[9] (please see in more detail below under questions 15 and 16).

---

5 Unofficial English translation of the Code of Criminal Procedure is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X60027K6&keel=en&pg=1&ptyyp=RT&tyyp=X&query=kriminaalmenetluse.

6 Unofficial English translation of the Surveillance Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30011K7&pg=1&tyyp=X&query=j%E4litustegevus&ptyyp=RT&keel=en.

7 Unofficial English translation of the Security Authorities Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X50038K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=julgeolekuasutus.

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

The national rules transposing the Directive do not contain specific rules on prohibiting the retention and/or transmission of sensitive data. The general rules on the protection of sensitive personal data are set out in the above referred Personal Data Protection Act10 and there are some other general rules that relate to the correspondence between attorneys and clients, but these are not designed to regulate the data retention regulation with particularity.

As regards correspondence between attorneys and clients, the Bar Association Act sets forth, inter alia, the following general principles: (i) information disclosed to an advocate shall be confidential;[11] (ii) media related to the provision of legal services by an advocate are intact;[12] (iii) an advocate is required to maintain the confidentiality of information which has become known to him or her in the provision of legal services, and the confidentiality of persons who request the advocate to provide legal services.[13] Reading these clauses in conjunction allows bringing the argument that any data regarding provision of legal services, including the data covered by the Directive, should be treated as confidential and should not be disclosed. However, it will remain to be seen, whether this argument will be followed and respected in practice.

---

8 Unofficial English translation of the Code of Civil Procedure is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X90041&keel=en&pg=1&ptyyp=RT&tyyp=X&query=tsiviilkohtu.

9 Unofficial English translation of the Securities Market Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40057K5&keel=en&pg=1&ptyyp=RT&tyyp=X&query=v%E4%E4rtpaberituru.

10 Unofficial English translation of the Bar Association Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30070K4&keel=en&pg=1&ptyyp=RT&tyyp=X&query=advokatuuri.

11 § 43(2) of the Bar Association Act.

12 § 43(5) of the Bar Association Act.

13 § 45(1) (first sentence) of the Bar Association Act.

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

Data are retained for one year since the start of communication if they are created during provision of communications services or are processed. Inquiries by surveillance agencies and security authorities and data given under those inquiries are retained for two years and the obligation to retain such data are on the applicant of the inquiry (§1111(4) of the ECA). For the purposes of public policy and national security these time limits can be extended by Government of Estonia for a limited time period (§ 1111(6) of the ECA). The law does not set out any more specific guidance or an absolute limit to this extension period.

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 ECA mandates the transfer of retained data explicitly only to surveillance agencies, security authorities, Financial Supervision Authority and courts (§ 1111(11) of the ECA).

Estonian surveillance agencies are: Estonian Security Police Board, Police and Border Guard Board, Military Police, Prisons Department of Ministry of Justice and prisons, Tax and Customs Board (§ 1 of Surveillance Act).

Estonian security authorities are: Security Police Board and Information Board (§ 5 of Security Authorities Act).

Private claimants or litigants cannot access the data retained directly, but they can ask the court to make requests to communications undertakings as part of the evidence collection procedure.

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

The national rules transposing the Directive do not contain specific rules on the purposes for which data retention can be used, with the exception of the provision which regulates providing of the retained data to the courts (§ 1141 of the ECA). Other legal acts contain additional grounds.

Code of Civil Proceedings – the law does not specify upon which conditions the court may decide to make the inquiry for retained data. According to the general rules of civil court proceeding, all parties have to provide evidence to prove their

claims and if they are unable to do so (e.g. in cases when they cannot get access to certain information), the participant in the proceeding may request the taking of the evidence by the court (§ 235(2) of Code of Civil Procedure). A participant in a proceeding who requests the taking of evidence must substantiate which facts relevant to the matter the participant in the proceeding wishes to prove by presenting the evidence or requesting the taking of evidence. A request for taking of evidence shall also set out any information which enables the taking of evidence (§ 235(3) of Code of Civil Procedure). It is under court's discretion to decide if there is a necessity to make an inquiry. As a general principle of the civil court proceedings, the court may accept, organise the collection of and consider, in adjudicating a matter, only evidence which has relevance to a matter ((§ 238 of Code of Civil Procedure). Hence, the decisive criterion is the relevance of the retained data for adjudicating the case.

Code of Criminal Proceedings – in criminal proceedings, collection of information concerning retained data is regarded as a surveillance activity. Using surveillance activities for collecting evidence is permitted if the collection of evidence by other procedural acts is precluded or especially complicated and the proceedings concern most serious crimes or crimes for which at least up to three years' imprisonment is prescribed as punishment. Additionally, it is also possible to collect information concerning retained data in proceedings related to offences, which are not severely punished, but which concern defamation, threatening, offences against minors, computer related offences and offences related to unpermitted disclosure of secrets (§§ 110 and 117 of the Code of Criminal Proceedings). The query to the communications undertaking can be presented by surveillance agency or security authority (§112 of the ECA), but the conducting of the surveillance activity as such must be authorised by a preliminary investigation judge's ruling upon reasoned request submitted by a prosecutor who directs the proceedings (§ 114(1) of the Code of Criminal Procedure).

Surveillance Act – in addition to the Code of Criminal proceedings, the Surveillance Act sets out reasons that justify commencement of surveillance proceedings (including accessing retained data) (§ 9(1) of the Surveillance Act). Such reasons are as follows:

1. the need to collect evidence in criminal proceedings;

2. evasion of a suspect or accused of a criminal proceeding or evasion of a convicted person of criminal punishment;

3. the need to collect information for the prevention and combating of criminal offences;

4. a person goes missing;

5. the need to decide on the access of a person to surveillance information or on permitting a person to work in a surveillance agency;

6. the need to perform security checks;

7. the need to decide upon the suitability of a police officer for police service or the suitability of persons who apply to the police service or to study on the police training programme;

8. the need to collect information for protection of witnesses;

9. the need to perform the obligations arising from international agreements and international conventions.

Moreover, the reason for the commencement of surveillance proceedings may be the need to decide on issuance of certain, if the agency competent to make the decision finds that the background or reliability of the applicant or information submitted by the applicant raise reasonable doubt, and if the alternative possibilities for verification thereof are exhausted (§ 9(2)-(3) of the Surveillance Act). Such licences include the following:

1. activity licence to work as a private detective;

2. an activity licence or operating permit for gambling;

3. an activity licence to engage in the provision of security services

4. an activity licence to an undertaking to engage in the areas of certain weapon-related activities;

5. a firearms procurement licence or a firearms licence to a citizen of a foreign state or a stateless person;

6. a residence or work permit or the grant of Estonian citizenship;

7. a licence or a General Export Authorisation User Certificate for the import, export or transit of strategic goods or provision of services related to military goods or entry of an undertaking in the state register of brokers of military goods.

If a reason for the commencement of surveillance proceedings exists, the surveillance proceeding is commenced by a reasoned decision made by the head of a surveillance agency or an official authorised thereof which is based on the following (§ 10(1) of the Surveillance Act):

1. an application from an investigative body or an order of a Prosecutor's Office in criminal proceedings;

2. an application from another surveillance agency;

3. an application from the head of the authority conducting the protection of witnesses an official authorised thereof;

4. an application from the other party to an international agreement entered into by Estonia, if so prescribed in the agreement;

5. an inquiry from Interpol or another international organisation, if the inquiry arises from the obligations of Estonia in the organisation;

6. an application from the head of an agency (except a surveillance agency) authorised to issue a licence or permit, as specified above.

Securities Market Act – in addition to the rules contained in the Code of Criminal Proceedings and Surveillance Act, the Securities Market Act sets out that the Financial Supervision Authority can inquire retained data from communications undertakings if there is reasonable doubt that certain infringements of Securities Market Act have taken place (§2303(2) of the Securities Market Act). In making such inquiries, the Financial Supervision Authority must fulfil the obligations of surveillance authorities. Moreover, such inquiries must be ordered by the member of the management board of the Financial Supervision Authority and authorised by the court pursuant to the rules of Code of Administrative Court Procedure[14] (§ 231 of the Securities Market Act).

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)?

Please see the answer to question 15.

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?

This depends on the proceedings in questions. In case of surveillance proceedings conducted under the Surveillance Act, there is no need for a court order. Please see also the answer to question 15.

There is no requirement to hear the aggrieved party or to involve him/her otherwise in the proceedings before data is accessed.

[14] Unofficial English translation of the Code of Administrative Court Procedure is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30054K9&keel=en&pg=1&ptyyp=RT&tyyp=X&query=halduskohtu.

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?

As a rule the information which becomes known to the communications undertaking in the process of provisions of communications services may be disclosed only to the relevant subscriber and, with the consent of the subscriber, to third persons, except in the cases specified in § 112, 113 and 1141 of ECA (these provisions provide the rights of surveillance agencies, security authorities and courts to get information about retained data or to require access to retained data).

In case of surveillance proceedings conducted under the Code of Criminal Proceedings and Surveillance Act, the agency which conducted surveillance activities must immediately give notification of the surveillance to the person with regard to whom the activities were conducted and the persons whose private or family life was violated by the activities (§ 121(1) of the Code of Criminal Proceedings and § 17(1) of the Surveillance Act). However, on the basis of a reasoned written decision made by the head of the surveillance agency or a person authorised by him or her, conduct of the surveillance activities need not be given notification of until the corresponding grounds cease to exist, if this may:

1. damage the rights and freedoms of another person which are guaranteed by law;

2. endanger the right of a person who has been recruited for surveillance activities to maintain the confidentiality of co-operation;

3. endanger the life, health, honour, dignity and property of an employee of a surveillance agency, a person who has been recruited for surveillance activities or another person who has been engaged in surveillance activities and of persons connected with them;

4. prejudice surveillance or a criminal proceeding or induce crime (§ 121(1) of the Code of Criminal Proceedings and § 17(1) of the Surveillance Act).

The person with regard to whom the activities were conducted and the person whose private or family life was violated by the activities has the right to examine the materials of the surveillance activities conducted with regard to him or her (§ 121(2) of the Code of Criminal Proceedings and § 17(2) of the Surveillance Act). Such examination is enabled upon the person's request. On the basis of a reasoned written decision made by the head of the surveillance agency or a person authorised by him or her, the following information need not be submitted for examination until the corresponding basis cease to exist:

1. information concerning the private life of other persons;

2. information which damages the rights and freedoms of another person which are guaranteed by law;

3. information which contains state secrets, secrets of another person or professional secrets of a surveillance agency;

4. information the submission of which may endanger the right of a person who has been recruited for surveillance activities to maintain the confidentiality of co-operation;

5. information the submission of which may endanger the life, health, honour, dignity and property of an employee of a surveillance agency, a person who been recruited for surveillance activities or another person who has been engaged in surveillance activities and of persons connected with them;

6. information the submission of which may prejudice a criminal proceeding and induce crime;

7. information which cannot be separated or disclosed without information specified above becoming evident (§ 121(2) of the Code of Criminal Proceedings and § 17(2) of the Surveillance Act).

In case of inquiries made under the Securities Market Act, the participants in proceedings have the right to access information concerning them which is collected by the Supervision Authority and to copy or make extracts of such information (§ 2313(2) of the Securities Market Act). The Supervision Authority has the right to refuse to submit information if this damages or may damage the legitimate interests of a third party or access to the information hinders or may hinder attainment of the objectives of supervision or may hinder the truth from being ascertained in criminal proceedings (§ 2313(2) of the Securities Market Act).

As regards civil proceedings, the law does not regulate the right to access data collected under civil proceedings. If the aggrieved party is not a party to the civil proceedings, its access to file of civil proceedings is rather limited in practice.

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

Please see the answer to the 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?

The national rules transposing the Directive do not contain specific rules on the recourse, but general rules on recourse to courts and remedies are contained in other

legal acts, such as the Code of Civil Proceedings, the Code of Criminal Procedure, the Surveillance Act, the Code of Administrative Court Procedure, the Administrative Procedure Act[15], the Securities Market Act and the State Liability Act[16].

In case of civil proceedings, this is not regulated. If the aggrieved party is a participant in the civil proceedings, he or she can make objection about the court's actions and dispute these in further appeal of the final judgement in case of an appeal is made to a higher instance court. If the aggrieved party is not a participant in the civil proceedings, there appears to be no recourse set out in the law.

In case of criminal proceedings, a participant in a proceeding or a person not participating in the proceeding has the right to file an appeal with the Prosecutor's Office against a procedural act or order of the investigative body if he or she finds that violation of the procedural requirements in the performance of the procedural act or preparation of the order has resulted in the violation of his or her rights (§ 228(1) of the Code of Criminal Proceedings). If the activities of an investigative body or Prosecutor's Office in violation of the rights of a person are contested and the person does not agree with the order prepared by the Public Prosecutor's Office who reviewed the appeal, the person has the right to file an appeal with the preliminary investigation judge of the county court in whose territorial jurisdiction the contested order was prepared or the contested procedural act was performed (§ 230(1) of the Code of Criminal Proceedings).

In case of surveillance activities, everyone may file a challenge with the head of a surveillance agency or the superior agency of the surveillance agency or submit a complaint to a Prosecutor's Office against the activities of the surveillance agency upon conduct of surveillance activities and everyone has the right of recourse to a court pursuant to the procedure prescribed by law if his or her rights and freedoms have been violated by a surveillance activity (§ 18 of the Surveillance Act).

If security authorities or the Financial Supervisory Authority have taken measures, which violate the rights of a person, the person may require an administrative authority or court to cancel or terminate the performance of a measure and to eliminate the consequences of the measure and compensate for the damages pursuant to the State Liability Act, and the person has recourse to an administrative court pursuant to the procedure prescribed in the Code of Administrative Court Procedure to seek protection of his or her rights (§ 109 of the Administrative Procedure Act).

Finally, the State Liability Act sets out that a person whose rights are violated by the unlawful activities of a public authority may claim compensation for damage caused

---

15 Unofficial English translation of the Administrative Procedure Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40071K3&keel=en&pg=1&ptyyp=RT&tyyp=X&query=haldusmenetluse.

16 Unofficial English translation of the State Liability Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X40075K2&keel=en&pg=1&ptyyp=RT&tyyp=X&query=riigivastutuse.

to the person, whereas both proprietary and non-proprietary damages could be claimed (§§ 7-9 of the State Liability Act).

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.

According to § 1111(9) of the ECA, upon retaining data, communications undertakings must ensure that:

a) the same quality, security and data protection requirements are met as those applicable to analogous data on the electronic communications network;

b) the data are protected against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

c) appropriate technical and organisational measures are taken to restrict access to the data;

d) no data revealing the content of the communication are retained.

Other than this provision, the ECA does not provide for any more particular ways.

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

This depends on the type of proceedings.

In civil proceedings, the law does not set out the obligation to destroy the data transmitted to the court. However, as a general principle, the court is to declare a proceeding or a part thereof (and the final judgement) closed on the initiative of the court or based on a petition of a participant in the proceeding if this is clearly necessary for the protection of the private life of a participant in a proceeding, witness or other person (§ 38 of the Code of Civil Procedure). This does not mean that the evidence must be destroyed, but it nevertheless means that the file where such information is contained cannot be accessed (§ 59(3) of the Code of Civil Procedure).In criminal proceedings, data recordings (such as photographs, films, audio and video recordings and other data recordings) necessary for the adjudication of a criminal matter and made in the course of surveillance activities must be stored in the criminal file or together with the criminal matter (§ 122(1), first sentence of the Code of Criminal Proceedings). The rest of the materials on surveillance activities must be stored in a surveillance file (§ 122(1), second sentence of the Code of Criminal Proceedings). The rules on the treatment of the information that is stored in the surveillance file are set of in §§ 161 and 162 of the Surveillance Act (see below). As data covered by the data retention obligation should by its nature not be qualified as "recording", it should not be added to the criminal file, but to the surveillance file.

If preservation of a data recording made in the course of surveillance activities and added to a criminal file is not necessary, the person subject to the surveillance activities or any other person whose private or family life was violated by such activities may request destruction of the data recording after the entry into force of the court judgment (§ 122(2) of the Code of Criminal Proceedings). In such case the law envisages destruction only upon the request of the person concerned. A body which conducted surveillance activities destroys a data recording at the request of a Prosecutor's Office and on the basis of an order of a preliminary investigation judge of a court which granted permission for the surveillance activities and in the presence of the prosecutor and the preliminary investigation judge (§ 122(3) of the Code of Criminal Proceedings).

Under the Surveillance Act, if initial information which was the reason for the commencement of the surveillance proceeding is not confirmed, the respective surveillance file must be destroyed after the closure of the file (§ 161(1) of the Surveillance Act). Other surveillance files must be destroyed after the expiry of the following retention periods:

1. surveillance files on criminal offences - until the expiry of the limitation period of the criminal offence;

2. personal surveillance files - until the redundancy of information contained therein, but for not longer than fifty years;

3. files on searching for missing persons - for twenty-five years after the entry into force of a court ruling concerning the declaration of death of the person;

4. other files on searching - for three years after the closure of the file (§ 161(2) of the Surveillance Act).

If preservation of a data recording made in the course of surveillance activities is not necessary, the person subject to the surveillance activities or any other person whose private or family life was violated by such activities may request destruction of the recording after the termination of the surveillance proceeding. Surveillance files subject to destruction and data recordings collected by surveillance activities must be destroyed by a committee which is formed by the head of a surveillance agency. The committee prepares a report concerning the destruction of a surveillance file and data recording collected by surveillance activities which must set out the number of the surveillance file or information concerning the destructed data recording and the reason for the destruction thereof (§ 162 of the Surveillance Act).

Dimension 2 (State – economy)

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

As noted in the answer to question 9, § 1111(1) of the ECA sets out general retention obligation on all communications undertakings. This obligation is only of general nature and is not referred to in other provisions of the ECA, which regulate quality, maintenance, use, etc. of the data to be retained under § 1111(2)-(3) of the ECA. Hence, under this clause all communications undertakings must retain data. The terms "communications undertaking" is defined as follows:

"electronic communications undertaking" (hereinafter communications undertaking) is a person who provides a publicly available electronic communications service[17] to the end-user or to another provider of a publicly available electronic communications service (§ 2, clause 5 of the ECA).

However, the more specific data retention obligations set out in § 1111(2)-(3) of the ECA are targeted with more particularity.

According to § 1111(2), certain obligations apply only to telephone service[18] or mobile telephone service[19] providers, while according to § 1111(3), certain obligations apply only to providers of Internet access, Internet e-mail and Internet telephony services. The latter three services (i.e. provision of Internet access, Internet e-mail and Internet telephony services) are not defined in the ECA or other laws.

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?

The ECA does not provide for such exceptions.

---

17 According to § 2, clause 6 of the ECA, "electronic communications service" is a service which consists wholly or mainly in the transmission or conveyance of signals on electronic communications networks under the agreed conditions. Network services are also electronic communications services.

18 According to § 2, clause 58 of the ECA, "telephone service" is a publicly available electronic communications service for originating and receiving national and international calls at a determined location and for access to emergency services through a number or a short access code connected with the number in the Estonian or international telephone numbering plan.

19 According to § 2, clause 31 of the ECA, "mobile telephone service" is a publicly available electronic communications service for originating and receiving national and international calls at an undetermined location and for access to emergency services through a number or a short access code connected with the number in the Estonian or international telephone numbering plan by establishment of partial or complete radiocommunication.

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?

Prior to the enactment of the Directive, the ECA did not oblige the data retention, but allowed the retention of certain data in the similar manner as now (e.g. for billing purposes or provisions of information society services). Please see more detailed overview of such regulation under the answer to question 10.

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 ECA does not set out additional rules, but the Personal Data Protection Act sets out general protections requirements.

Processing of personal data is regulated by the Personal Data Protection Act that regulates processing and using of personal data of private individuals.

According to Personal Data Protection Act, processing of personal data means any act performed with personal data, including the collection, recording, organisation, storage, alteration, disclosure, granting access to personal data, consultation and retrieval, use of personal data, communication, cross-usage, combination, closure, erasure or destruction of personal data or several of the aforementioned operations, regardless of the manner in which the operations are carried out or the means used (§ 5 of the Personal Data Protection Act).

A processor of personal data means the entity or person who processes personal data or on whose assignment personal data is processed (§ 7(1) of the Personal Data Protection Act). It is up to the processor of personal data to determine: (i) the purposes of processing of personal data; (ii) the categories of personal data to be processed; (iii) the procedure for and manner of processing personal data; (iv) permission for communication of personal data to third persons (§ 7(2) of the Personal Data Protection Act). A processor of personal data (chief processor or controller) may authorise, by a contract, another person (authorised processor) to process personal data (§ 7(3) of the Personal Data Protection Act). In such case the chief processor (controller) has to provide the authorised processor with mandatory instructions for processing personal data and the chief processor (controller) remains responsible for the authorised processor's compliance with the personal data processing requirements. The chief processor (controller) determines the requirements specified in (i)-(iv) above for the authorised processor (§ 7(4) of the Personal Data Protection Act). The authorised processor may delegate the task of processing personal data to another person only with the written consent of the chief processor (controller), provided that this does not exceed the limits of the authority of the authorised processor (§ 7(5) of the Personal Data Protection Act).

The basic principles of data protection are set out in § 6 of the Personal Data Protection Act. Accordingly, any processor of personal data (both chief and authorised processors) must always to adhere to the basic following principles:

1. principle of legality – personal data can collected only in an honest and legal manner;

2. principle of purposefulness – personal data can be collected only for the achievement of determined and lawful objectives, and such data cannot be processed in a manner not conforming to the objectives of data processing;

3. principle of minimalism – personal data can be collected only to the extent necessary for the achievement of determined purposes;

4. principle of restricted use – personal data can be used for other purposes only with the consent of the data subject or with the permission of the competent authority;

5. principle of high quality of data – personal data has to be up-to-date, complete and necessary for the achievement of the purpose of data processing;

6. principle of security – security measures have to be applied in order to protect personal data from involuntary or unauthorised processing, disclosure or destruction;

7. principle of individual participation – the data subject has to be notified of data collected concerning him or her, the data subject has to be granted access to the data concerning him or her and the data subject has the right to demand the correction of inaccurate or misleading data.

Processing of any personal data is generally allowed only upon the consent of the data subject (§ 10(1) of the Personal Data Protection Act). According to § 14(1) of the Personal Data Protection Act, processing of personal data is permitted without the consent of a data subject if the personal data is to be processed:

1. on the basis of law;

2. for performance of a task prescribed by an international agreement or directly applicable legislation of the Council of the European Union or the European Commission;

3. in individual cases for the protection of the life, health or freedom of the data subject if obtaining the consent of the data subject is impossible;

4. for performance of a contract entered into with the data subject or for ensuring the performance of such contract unless the data to be processed is sensitive personal data.

According to § 14(2) of the Personal Data Protection Act, communication of personal data or granting access to personal data to third persons for the purposes of processing is permitted without the consent of the data subject:

1. if the third person to whom such data is communicated processes the personal data for the purposes of performing a task prescribed by law, an international agreement or directly applicable legislation of the Council of the European Union or the European Commission;

2. in individual cases for the protection of the life, health or freedom of the data subject if it is impossible to obtain the consent of the data subject;

3. if the third person requests information obtained or created in the process of performance of public duties and the data requested does not contain any sensitive personal data and access to it has not been restricted for any other reasons.

If the source of personal data is any other than the data subject himself or herself, then after obtaining or amending of the personal data or communicating the data to third persons, the processor of the personal data must promptly inform the data subject of the content and source of the personal data to be processed together with the details of the processor (§ 15(1) of the Personal Data Protection Act). Nevertheless, a data subject need not be informed of the processing of his or her personal data obtained from another source than the data subject himself or herself:

1. if the data subject has granted consent for the processing of his or her personal data;

2. if the data subject is aware of the source of the personal data and is aware of the content of the data processed, as well as of the details of the processor;

3. if processing of the personal data is prescribed by law, an international agreement or directly applicable legislation of the Council of the European Union or the European Commission;

4. if informing of the data subject is impossible;

5. if informing of the data subject would damage rights and freedoms of other persons, endanger the protection of the confidentiality of paternity or maternity of a child, hinder the prevention of a criminal offence or apprehension of a criminal offender, complicate the ascertainment of the truth in a criminal proceeding (§ 15(2) and § 20(1) of the Personal Data Protection Act).

27. **Which additional costs (i.e. costs over and above those arising from the retention of the data categories specified in your answer to question 25) originate in total from the implementation of the national law transposing the Directive (i.e. aggregate figures of all obligated parties in your country as a whole)?**

According to a survey conducted by Ministry of Economic Affairs and Communication on the estimated costs of data retention before adopting the Directive into Estonian law[20], it was calculated that if the requirements of the Directive were applied to all obligated communications undertakings then it would require investments in the amount of approximately EEK 500 million to 1.2 billion (EUR 32-72 million) and annual fixed costs would be EEK 300-600 million (EUR 19-28 million). We are not aware of surveys on the actual costs connected to the implementation of the Directive required from communications undertakings. The costs related to costs arising from retaining or processing of data is not compensated to the communications undertakings.

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

The costs related to costs arising from retaining or processing of data is not compensated to the communications undertakings (§ 1111(10) of the ECA).

However, communications undertakings are compensated for the costs incurred in relation to the provision of the information to surveillance agencies or security authorities out of the state budget fees sector through the budget of the ministry in the area of government of which the surveillance agency or security authority belongs. Such costs are compensated in accordance with the agreement entered into between the surveillance agency or security authority and the communications undertaking (§ 114 of the ECA).

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

If a surveillance agency or a security authority is making an inquiry, then in case of urgent inquiries, the communications undertaking is obliged to give information about the retained data at the first opportunity, but not later than in 10 hours and in case of other cases not later than in 10 working days, if following the previously mentioned deadlines is possible according to the content of the inquiry (§ 112(1) of the ECA). The inquiry must be submitted in writing or by electronic media or made in oral form verifying the request with a password. Access to the data may also be

[20] Available: http://www.mkm.ee/failid/Telekommunikatsiooni_andmete_s_ilitamise_v_imalike_kulude_anal__s_2.91556.doc (only in Estonian).

granted online on the basis of a written contract (§ 112(2) of the ECA). Providers of mobile services must enable the localisation of terminal equipment in real time to surveillance agencies or a security authorities on the basis of a written agreement (§ 112(3) and (4) of the ECA).

In addition to the obligation related to data retention the ECA regulates also giving access to communications network to surveillance agencies and security authorities, which relates to restricting the right to secrecy of messages and conduction of other surveillance activities (§ 113 of the ECA).

According to § 1141 of the ECA, communications undertakings have an obligation to provide information to courts on the basis of a single written inquiry thereof within the term specified by the court.

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.

Violation of the data retention obligation is punishable by a fine of up to 300 fine units, i.e. up to EEK 18,000 (EUR 1150), on natural persons and by a fine of up to EEK 50,000 (EUR 3,200) on legal persons (§ 1841 of the ECA).

Violation of the obligation to provide information and guarantee access to communications networks to surveillance agencies and security authorities is punishable by a fine of up to 200 fine units, i.e. up to EEK 12,000 (EUR 767) on natural persons and by a fine of up to EEK 40,000 (EUR 2,500) on legal persons (§ 185 of the ECA).

The law does not set out specific sanctions with regard to a violation of *data protection and data security rules* in the context of data retention. The Personal Data Protection Act sets out that officials of the Data Protection Inspectorate have the right to issue precepts to processors of personal data and adopt decisions for the purposes of ensuring compliance with the Personal Data Protection Act (§ 40(1) of the Personal Data Protection Act). Upon failure to comply with such a precept, the Data Protection Inspectorate may impose a penalty payment of up to EEK 150,000 (EUR 9,587) (§ 40(2) of the Personal Data Protection Act). Penalty payment cannot be imposed on state agencies (§ 40(2) of the Personal Data Protection Act). If a state agency who is the processor of personal data fails to comply with the precept of the Data Protection Inspectorate within the term specified therein, then the Data Protection Inspectorate may file a protest with an administrative court pursuant to procedure provided for in the Code of Administrative Court Procedure (§ 40(4) of the Personal Data Protection Act).

Violation of the requirements regarding security measures to protect personal data or violation of other requirements for processing of personal data prescribed in the Personal Data Protection Act, if a precept issued to the person by the Data Protection Inspectorate on the basis of § 40 of the Personal Data Protection Act for the elimination of the violation is not complied with, is punishable by a fine of up to

300 fine units, i.e. up to EEK 18,000 (EUR 1150) on natural persons and by a fine of up to EEK 500,000 (EUR 32,000) on legal persons ((§ 43 of the Personal Data Protection Act).

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?

Entitled bodies (surveillance agencies, security authorities, Financial Supervisory Authority and courts) establish the contact and make an inquiry about relevant information themselves.

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

No.

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

General principles and practices of co-operation between different investigative bodies such as different surveillance agencies and security authorities existed already before the transposition of Directive. These principles and practices were not significantly affected by the transposition of the Directive. The details of such principles or practices are generally not publicly available.

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 to (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 processing of (responses to) incoming requests?

The obligated parties are not entitled to exchange retained data directly with any foreign state bodies. It is possible to exchange data on the basis of mutual assistance treaties or arrangements (e.g. between the EU Member States' authorities or under Convention on Cybercrime as Estonia is a party to it, cooperation agreement between Estonia and Hungary concerning terrorism, illicit drug trafficking and the fight against organized crime, the UN Convention against organised crime, the UN Convention for the Suppression of Financing of Terrorism, the European Convention for the Suppression of Terrorism, Council of Europe Convention on the

Prevention of Terrorism, the Bilateral Treaty Between Estonia and USA on Mutual Legal Assistance in Criminal Matters), but such requests should not be submitted to Estonian communications undertakings directly, but only to through relevant Estonian authorities.

Such requests should be sent to the Estonian Ministry of Justice, which is the designated central authority responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. The Estonian Police and Border Control Board is the further point of contact.

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

The monitoring of compliance over the communications undertakings' obligation to retain data is performed by the Technical Surveillance Authority, which is a governmental organisation operating in the administrative area of the Ministry of Economic Affairs and Communications. The monitoring of the communications undertakings' obligation to provide information to surveillance agencies and security authorities is performed by police authorities or by Security Police Board. In case of non-compliance by a communications undertaking, respective authorities can issue administrative injunctions requiring compliance or conduct misdemeanour proceedings and impose fines for non-compliance in the amount set out in the answer to question 30.

The supervision over the activities of surveillance agencies and security authorities is performed by the Prosecutor's Office and Security Authorities Surveillance Select Committee of the *Riigikogu* (The Parliament of Estonia). The Prosecutor's Office is a government agency within the administrative area of the Ministry of Justice. According to the Prosecutor's Office Act[21], the Prosecutor's Office participates in planning surveillance required for the prevention and detection of crimes; leads pre-trial criminal proceedings ensuring its lawfulness and effectiveness; and represents public prosecution in court and fulfils other duties imposed on the Prosecutor's Office by law. The Security Authorities Surveillance Select Committee of the *Riigikogu* exercises supervision over the legality of surveillance and the activities of the Security Police. The Committee monitors the conformity of the activities of the Security Police Board with the Constitution, the Surveillance Act and numerous other legal acts, and the compliance of the activities of the Police Board, the Border Guard Administration, the General Staff of the Defence Forces, the Prison Board

[21] Unofficial English translation of the Prosecutor's Office Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X2050K10&keel=en&pg=1&ptyyp=RT&tyyp=X&query=prokuratuuriseadus.

and the Customs Board with the Surveillance Act. The authority of the Committee ends at the termination of the authority of the present *Riigikogu*.

The law does not set out specific regulation with regard to a violation of *data protection and data security rules* in the context of data retention. As noted above under answer to question 30, the Personal Data Protection Act sets out that officials of the Data Protection Inspectorate have the right to issue precepts to processors of personal data and adopt decisions for the purposes of ensuring compliance with the Personal Data Protection Act (§ 40(1) of the Personal Data Protection Act). The Data Protection Inspectorate is independent in its activities under the Personal Data Protection Act. The head of the Data Protection Inspectorate is appointed by the government after having heard the opinion of the Constitutional Committee of the *Riigikogu*. The head of the Inspectorate may be released by the government on the proposal of the Minister of Justice, in some cases after having heard the opinion of the Constitutional Committee of the *Riigikogu*.

II. Relevant case-law

36. Are there any lawsuits or administrative proceedings – pending or concluded by a final adjudication – concerning the legality of the national law transposing the Directive or parts thereof?

If so, please answer to the following questions:

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

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

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

We are not aware of such lawsuits.

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

We are not aware of such 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?

The law does not explicitly set out where the data are to be stored. According to the Regulation No. 56 of the Minister of Economic Affairs and Communication of 25 June 2008 "The procedure for retention, passing over to the Technical Surveillance Board, deleting and destroying data, inquiries, log files and applications" undertakings must apply appropriate measures to ensure the storage of data in compliance with the ECA. The aforementioned regulation provides that the undertakings must store log files and applications in a guarded room with restricted access and store log files in such a manner that makes it possible to the handle log files concerning the actions performed by the central surveillance device according to time, type, object and number of action for a period of at least five years.

There is no information about the practice of undertakings regarding the matter, other than in 2008 there were many deficiencies as to the storage of data by the undertakings. Furthermore, in 2008 all the undertakings had different methods of storing data, but such discrepancies and deficiencies were supposed to be tackled with the abovementioned Regulation No. 56.

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

The data that is retained under § 1111(2) and (3) of the ECA (i.e. the data listed in Art. 5 of the Directive) must be retained in the territory of an EU Member State. The data concerning the authorities' or courts' inquiries must be retained in the territory of Estonia (§ 1111(5) of the ECA).

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

a) no data are retained beyond what is permitted?

The law does not set out explicit regulation on this aspect. Hence, this is left for each communications undertaking to procure.

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)?

Depending on the procedure and issue at hand, the supervision may be exercised by the Prosecutor's Office, courts or the Security Authorities Surveillance Select Committee of the *Riigikogu*. The latter exercises supervision over agencies of

executive power in questions relating to the activities of security authorities and surveillance agencies, including ensuring of fundamental rights and efficiency of the work of security authorities and surveillance agencies, and in questions relating to supervision exercised thereover. The committee submits an overview of the activities of the committee and the results thereof to the *Riigikogu* at least once a year. If an offence is detected, the committee is required to forward the relevant materials to an investigative body or the Chancellor of Justice (§ 36 of the Security Authorities Act).

We are not aware of any legal or illegal technical interfaces enabling state bodies to access the retained data directly.

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

Please see the answer to the previous question.

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 Regulation No. 56 of the Minister of Economic Affairs and Communication of 25 June 2008 "The procedure for retention, passing over to the Technical Surveillance Board, deleting and destroying data, inquiries, log files and applications" provides for several technical and organisational measures, which ensure that no data are retained beyond what is permitted. According to the referred regulation, while retaining log files and applications, communications undertakings must designate persons who have access to log files and applications; register the time when log files and applications were accessed; retain the data in premises with limited access and surveillance; and notify the Security Authorities Surveillance Select Committee of the *Riigikogu*, Prosecutor's Office and the Technical Surveillance Board of disturbances in the data retention process. Communications undertakings must notify the Security Police Board of all the names, contact data and personal identification codes of persons who have access to retained data.

The ECA sets out fines only for the violation of the obligation to store log files and applications in compliance with ECA - fine up to EEK 18 000 (EUR 1150) on natural persons and up to EEK 50,000 (EUR 3,200) on legal persons (§ 1841 of the ECA). The violation of the obligation to maintain the confidentiality of information concerning a user which becomes known in the process of provision of communications services is punishable by a fine of up to 200 fine units, i.e. up to EEK 12,000 (EUR 767) on natural persons and up to EEK 50,000 (EUR 3,200) on legal persons (§ 1842 of the ECA).

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

According to § 2(3) of the Regulation No. 56 of the Minister of Economic Affairs and Communication of 25 June 2008 "The procedure for retention, passing over to the Technical Surveillance Board, deleting and destroying data, inquiries, log files and applications", a commission created by the Technical Surveillance Authority, which consists of representatives of the Technical Surveillance Authority, the Public Prosecutor's Office, the Security Authorities Surveillance Select Committee of the *Riigikogu* and the Security Police Board, supervises the destroying of data and controls that data are destroyed safely.

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

The law does not set out specific technical measures for this. However, the law sets out a general proceeding in case any surveillance activities are conducted under the Surveillance Act. Accordingly, the person with regard to whom the activities were conducted and the person whose private or family life was violated by the activities has the right to examine the materials of the surveillance activities conducted with regard to him or her. Such information may be disclosed for access only in the offices of the surveillance agency and, if possible, it should be presented in a systemised manner and chronologically (§ 172(1) of the Surveillance Act).

A report must be prepared concerning the access to information and the report must set out the type, number and date of preparation of each document disclosed for the access and the number of pages. The person who accessed the information and the official(s) who disclosed such information for access must sign the report. If the person who accessed the information refuses to sign the report, the official is to make a notation to that effect in the report and confirm it by his or her signature. The head of the corresponding surveillance agency must approve the standard format for reports on the access to information (§ 172(2)-(4) of the Surveillance Act).

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

As noted in the answer to question 12, the national rules transposing the Directive do not contain specific rules on prohibiting the retention and/or transmission of sensitive data. The general rules on the protection of sensitive personal data are set out in § 25 of the Personal Data Protection Act.

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)?

The law does not provide further measures in addition to the measures described under previous questions.

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?

Please see the answer to question 21.

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.

Please see the answer to question 21.

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?

Please see the answer to question 34.

As regards the common working language in this context, most of Estonian officials are sufficiently proficient in English and most of foreign correspondence is handled in English. In addition, depending on the authority and the official handling the matter, Russian may be used as a working language to handle inquiries for instance from Russia or other CIS countries.

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 some discussion in the media, when the transposition was prepared and there were both proponents and opponents of data retention represented in the media. In general, the discussion was rather mild. It is not possible to clearly distinguish the view-points of different social and political groups, as the debate over data retention issues was not that large-scale. Nevertheless, there are some examples of organisations that had an opinion concerning the transposition of the Directive. For example, the Estonian Bar Association expressed their concern over the issue that the Directive might endanger the professional confidentiality requirement of attorneys and the right to defence, which among other aspects entails that the very fact of contacting an attorney is confidential.

Overall, it can be said that Estonian public do not have a very strong opinion concerning the data retention issues. Of course, the opponents have brought out arguments that people are losing their right to privacy and that state has too many ways to interfere in people's private sphere, but in general, it does not seem to be a major concern for Estonian society.

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)?

The Maritime Safety Act sets out an obligation to keep passenger lists in case of passenger ships (except on passenger ships operating on domestic voyages or navigating in Estonian inland waters). The list must contain the name, date of birth, citizenship or country of residence and gender of the passenger and the route of the ship.

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.

We are not aware of such statistics or evaluations being publicly available.

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

We are not aware of such information being publicly available.

49. Are there any discussions going on in your country to expand/narrow down the categories of data to be retained, their retention period or their purposes of use?

There is currently no active discussion going on in Estonia on the scope of data to be retained, the retention periods or purposes of use. However, draft amendments to the ECA are pending, which *inter alia* envisage stricter obligations on the protection of personal data on communications undertakings. The amendments stipulate obligation to notify about the infringements of personal data protection and the procedure for notification thereof to the Data Protection Inspectorate. The infringement of personal data protection will be defined as the infringement of security obligations which would cause accidental or unlawful destruction, loss, change, unlawful publication or access to data transmitted, stored or handled in another manner upon provision of communication services.

Furthermore, the amendments will provide that costs regarding hardware and software used to enable the surveillance agency or security authority access to a communications network are to be borne by the communications undertaking instead of the government. However, this does not concern data retention, but only access devices.

The referred draft amendments and explanatory memorandum to the amendments are available on the website of Riigikogu, but only in Estonian (http://www.riigikogu.ee/?page=eelnou&op=ems&emshelp=true&eid=1212775&u=20101228120424).

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

Fundamental rights are set out in the 2nd chapter of the Estonian Constitution[23]. According to § 26 of the Constitution, everyone has the right to the inviolability of private and family life. State agencies, local governments and their officials must not interfere with the private or family life of any person, except in the cases and pursuant to procedure provided by law to protect health, morals, public order, or the rights and freedoms of others, to combat a criminal offence, or to apprehend a criminal offender. § 43 of the Constitution provides that everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means.

There are also several other fundamental rights, which could be affected by data retention. For instance, § 15 of the Constitution set out that everyone whose rights and freedoms are violated has the right of recourse to the courts; § 19 provides the right to free self-realisation; § 29 provides freedom to choose his or her area of activity, profession and place of work; § 40 provides freedom of conscience, religion and thought; § 41 provides the right to remain faithful to his or her opinions and beliefs; § 44 provides freedom to obtain information disseminated for public use, etc.

The Constitution does not contain explicit reference to the data or its retention in the electronic communications context. The Estonian Supreme Court has not analyzed the question, whether it is legal under Estonian constitutional law to retain this

---

22 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).

23 Unofficial English translation of the Constitution is available at: http://www.legaltext.ee/et/andmebaas/paraframe.asp?loc=text&lk=et&sk=en&dok=X0000K1.htm&query=põhiseadus&tyyp=X&ptyyp=RT&pg=1&fr=no.

content without a specific reason; therefore no firm opinion can be formed on the views of Estonian higher courts.

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 general, rights and freedoms may be restricted only in accordance with the Constitution and only on the basis of legal acts, as is the case with the ECA and other legal acts referred to above. Such restrictions must be necessary in a democratic society and must not distort the nature of the rights and freedoms restricted (§ 11 of the Constitution).

Exceptions to the right to confidentiality of messages may be made by court authorisation to combat a criminal offence, or to ascertain the truth in a criminal procedure, in the cases and pursuant to procedure provided by law (§ 43, 2nd sentence of the Constitution).

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?

We are not aware of such case law in Estonia.

53. Does national (constitutional) law safeguard an absolute limit as to the maximum degree to which public surveillance measures collectively may restrict fundamental rights, or has an assessment/balance of interests to be carried out in each individual case?

There is no absolute limit or maximum degree to which public surveillance measures may collectively restrict fundamental rights; the assessment of balance of interests is carried out in each individual case.

54. Does national (constitutional) law require that exemptions be provided for from the obligation to retain or to transmit certain data that are worth being protected (cf. question 12)?

There are no such explicit exceptions in the Constitution.

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?

There has not been active academic discussion on this issue and the Estonian Supreme Court has not analyzed whether the restrictions are in line with the Constitution. Therefore, it is rather hard to establish the general opinion of the Estonian legal community on whether the data retention obligation is in accordance with the Estonian Constitution. Private undertakings may or must assist law enforcement agencies according to relevant laws or court orders. There is no special regulation in the Constitution, although freedom of establishment or business, professional freedom, fair competition might be affected. However, it is common to put certain obligations to private undertakings. It could be argued that the aforementioned data retention obligations are not excessively restrictive or discriminative taking into account the technical possibilities and the number of undertakings affected, although the question of compensation and extra funds needed for performing the duties may arise. The Supreme Court may declare such regulations unconstitutional if they infringe any fundamental 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)?

One of the purposes of data retention is establishing the truth in civil proceedings. There are various other means that can be used for this purpose within the context of collecting evidence in civil proceedings, including use of expert witnesses, who could be private actors.

Generally, only public authorities are entitled to enforce law. However, under some circumstances, bailiffs could also be regarded as law enforcers. Bailiffs operate under established statutory framework, but are nevertheless private actors. Such obligations may derive from law. The obligation to assist law enforcement agencies, the government or local governments is not regulated in a single act but the obligations are set by different laws concerning the relevant field. Therefore, the data retention obligation is governed by the ECA and related government regulations which provide the conditions and requirements for data retention. There are no limits as to the possibility of obliging private actors to engage in public matters, but fundamental principles of the Constitution must be observed.

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

The Constitution does not explicitly contain such an obligation.

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?

In the Estonian hierarchy of norms, international treaties, including ECHR, are above national legal acts. If there is a conflict between a provision of an international treaty and a national legal act, the provision of an international treaty should prevail. The Constitution takes preference to international treaties, the international treaties that are not in compliance with the Constitution are not applied. According to the Constitution, the government may not enter into an agreement if it is contrary to the Constitution. If there is a conflict between an international treaty and the Constitution, the conflict should be solved by interpretation of the Constitution by the Supreme Court.

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?

The status of the EU directives vis-à-vis Estonian legal system is regulated by the EU law, and there is not much room for significantly differing interpretations as regards the immediate effect.

The process of transposing an EU directive into Estonian national law can be divided into two parts. Firstly, implementing legislation is prepared by a competent ministry and proceeded in *Riigikogu*. Secondly, the European Commission must be notified of the implementing legislation. As a rule, the ministry, who was responsible for participating in the proceedings preceding the adoption of the directive at the Council, is also responsible for drawing up the legislation for transposing the directive.

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?

Prior to joining the EU, an amendment to the Estonian Constitution was passed. According to § 1 of the Constitution of the Republic of Estonia Amendment Act[24],

[24] Unofficial English translation of the Constitution of the Republic of Estonia Amendment Act is available at:

Estonia may belong to the EU in accordance with the fundamental principles of the Constitution. Further, § 2 provides that as of Estonia's accession to the EU, the Constitution applies taking account of the rights and obligations arising from the Accession Treaty.

The Estonian Supreme Court has expressed in its opinion[25] that pursuant to the Constitution of the Republic of Estonia Amendment Act and EU law, in case of conflict between Estonian law and EU law, the latter will be applied even if EU law is not in accordance with the Estonian Constitution. Only these provisions of the Constitution can be applied, which are in accordance with EU law or which are not regulated by EU law. The Supreme Court did not analyse the relationship between § 1 and § 2 of the Constitution of the Republic of Estonia Amendment Act. However, the Supreme Court ruling, according to which EU law takes preference to the Constitution, has been criticised in the dissenting opinion of two justices. The ruling is criticised to have not analysed § 1 of the Amendment Act and unjustifiably broadened the supremacy of EU law even further than it has been done by the ECJ rulings. Commentary to the Constitution[26] bases the preference of EU law in addition to the Supreme Court ruling also on the ECJ judgment of 12 December 1970 in case C-11/70 (Internationale Handelsgesellschaft), according to which the courts of Member States may not ignore EU regulations even if they are not in compliance with the constitution of the Member State. Commentary adds that § 1 of the Constitution of the Republic of Estonia Amendment Act does not stipulate the fundamental principles, which might be the principles without which Estonia and the Constitution lose its essence. According to the Commentary, it is considered that EU law is applicable even if not in compliance with the Constitution. There has not been any important academic or political discussion to provide more insight into the matter. At the moment, the Supreme Court's ruling is the basis for the interpretation of the Constitution and its relationship with the EU law.

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

As can be concluded on the basis of the answers to the previous questions, there are several authorities and ministries involved in different aspects related to data retention, including the Technical Surveillance Authority, the Financial Supervisory Authority, surveillance agencies and security authorities, the Prosecutor's Office, court, the Ministry of Justice, the Ministry of Economic Affairs and the

---

http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X70050&keel=en&pg=1&ptyyp=RT&tyyp=X&query=p%F5hiseadu.

25 Available at: http://www.nc.ee/?id=11&tekst=222488463 (only in Estonian).

26 Truuväli, E.-J., et al.; Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, Tallinn: Juura, Õigusteabe AS, 2008.

Communications and the Security Authorities Surveillance Select Committee of the Riigikogu. Their competences have been discussed above.

As Estonia is not federal state, there is no split of competence between the states' authorities and the federal authorities.

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

The Constitution does not contain explicit limits regarding the transmission of retained data to other countries.

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?

As the regulation relating to data retention is rather new, it is hard to make conclusions on the main shortcomings and problems of the regulation yet. However, as the regulation of the rights data subjects, the obligations of communications undertakings and the competences of different authorities entitled to access retained is contained in numerous different legal acts and the competences are shared by several agencies and authorities, the overall regulation is rather difficult to comprehend. Furthermore, there are some inconsistencies between the different legal acts, which further complicate understanding and determining the scope of rights and obligations of various participants involved. The regulations provide for security and confidentiality of the data stored by the undertakings, however, more precise and constant state supervision of the application of these regulations may improve and guarantee the security of privacy. Moreover, the both the data subject and the law enforcer would benefit from more straightforward and better structured rules than currently in force.

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

Estonia

Pirkko-Liis Harkmaa, LAWIN

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 specific provision in the Constitution regarding anonymous communication.

Paragraph 26 of the Constitution of the Republic of Estonia stipulates that everyone has the right to the inviolability of private and family life. State agencies, local governments and their officials must not interfere with the private or family life of any person, except in the cases and pursuant to procedure provided by law to protect health, morals, public order, or the rights and freedoms of others, to combat a criminal offence, or to apprehend a criminal offender.

Further, § 43 of the Constitution provides that everyone has the right to confidentiality of messages sent or received by him or her by post, telegraph, telephone or other commonly used means. Exceptions may be made by court authorisation to combat a criminal offence, or to ascertain the truth in a criminal procedure, in the cases and pursuant to procedure provided by law.

Thus, the Constitution only sets out the general right to the privacy of family and private life and to confidentiality of messages, but does not specifically provide the right to communicate anonymously.

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?

On 22 February 2011, the amendments in the Electronic Communications Act (ECA, the law that inter alia sets out the data retention obligation) were adopted. Most of these amendments entered into force on 25 May 2011. The amendments mostly related to radio frequencies, numbering, the international co-operation of the electronic communications market regulator, SMP and universal service regulation, but also personal data protection.

According to the new provision regarding the personal data protection (1021 of the ECA), the violation in connection with the protection of personal data is regarded as the infringement of security obligations which results in the accidental or illegal destruction, loss, change or illegal disclosure of or access to personal data that has been transmitted, stored or processed in any other manner in the course of providing communication services. In case of violation in connection with the protection of personal data, the communication undertaking must notify the Data Protection Inspectorate. If the violation may affect the personal data or inviolability of private life of client or end-user, whose data has been submitted to the communication undertaking by the client, then the communication undertaking must notify the client as soon as possible of at least the following: the description of the infringement related to personal data, contact information for further information, and recommendations to alleviate the adverse effects of the infringement. The communications undertaking does not have to notify the client about the violation, if it has proven to the Data Protection Inspectorate that appropriate technological protective measures were applied prior to the infringement. Such measures must procure that the data in question is made illegible for all unauthorised persons. However, even in such case the Data Protection Inspectorate may require the notification of the client taking into account the seriousness of the effect of the infringement. Finally, communications undertakings must keep track of the violations related to personal data (including at least the description of the violation and its possible adverse effects and the overview of technological protective measures taken to end the violation.

Moreover, a package of amendments regarding surveillance activities in general was adopted on 17 February 2011 (the text of the Act on Amending the Code of Criminal Procedure and Other Acts is available in Estonian at: https://www.riigiteataja.ee/akt/121032011002, no English text of this act is available). These amendments abolish the Surveillance Activities Act and incorporate its provisions into text of the Code of Criminal Procedure, and at the same time make related amendments to various other legal acts. Generally, the purpose of this package is to clarify and organise the regulation of surveillance activities and to implement better supervision of surveillance activities. According to the amendments, surveillance activities may be conducted on the basis of a written authorisation of a preliminary investigation judge or in certain cases and in urgent matters the authorisation of the Prosecutor's Office is required. In case of data retention the permission of the Prosecutor's Office is needed. These

amendments should enter into force on 1 January 2012. However, these amendments have been attacked by the legal chancellor and legal community and it is possible that these will be reviewed before the entry into force. Nevertheless, at the moment no plans to change the future regulation have been made.

To the best of our knowledge, there are no specifically data retention related amendments pending at the moment. According to ECA all the data is preserved for one year regardless of the specific application to preserve certain data about a specified subject. The data that has been forwarded to surveillance authority on the basis of a specified application must be preserved by that authority for two years. There are no other models (e.g. quick-freeze) being discussed in Estonia at the moment.

3. **In which way and to which extent are private actors (citizens, undertakings) generally obligated in your country, by means *other* than data retention, to co-operate with public authorities in the detection, investigation and prosecution of criminal offences and/or for any other of the legitimate purposes for which providers are (also) obligated to retain data?**

Private actors, such as members of certain occupations, may have some data retention obligations. For example, health care providers, who have the obligation to maintain confidentiality arising from law, have the right to process personal data required for the provision of a health service, including sensitive personal data, without the permission of the data subject. Notaries have the obligation to maintain certain data. However, the general rule is that private actors are obliged to report only if they become aware of a first degree criminal offence.

4. **Which rules governing the rights of persons (e.g. in specific circumstances such as a lawyer) to refuse to testify/to deliver evidence against themselves (in court) do exist in the national law of your country? Do these rules include (according to their wording or according to the meaning identified through applying commonly used methods of interpretation) data that is to be retained and – as the case may be – transmitted under the national law transposing Directive 2006/24/EC on data retention (hereinafter: "the Directive")? Do these rights to refuse to testify conflict with data retention in a way that they bar these data from being retained, transmitted and/or used as an evidence in court?**

The general rights of witnesses in criminal proceedings are stipulated in § 71-73 of the Code of Criminal Procedure. We have cited these provisions in the footnote for your information.[1] However, these do not contain any specific regulation or wording on the data that is to be retained according to data retention regulation.

---

[1] According to § 71, the following persons have the right to refuse to give testimony as witnesses:
1) the descendants and ascendants of the suspect or accused;
2) a sister, stepsister, brother or stepbrother of the suspect or accused, or a person who is or has been married to a sister, stepsister, brother or stepbrother of the suspect or accused;
3) a step or foster parent or a step or foster child of the suspect or accused;
4) an adoptive parent or an adopted child of the suspect or accused;
5) the spouse of or a person permanently living together with the suspect or accused, and the parents of the spouse or person, even if the marriage or permanent cohabitation has ended.

According to § 91 of the Code of Criminal Procedure a notary's office or an attorney's law office must be searched in the presence of the notary or attorney. If the notary or attorney cannot be present at the search, the search must be conducted in the presence of the person substituting for the notary or another attorney providing legal services through the same law office, or if this is not possible, any other notary or attorney.

Furthermore, § 43(2) of the Bar Association Act states that an attorney or employee of the Bar Association or a law office who is being heard as a witness may not be interrogated or asked to provide explanations on matters that he or she became aware of in the course of provision of legal services. The same paragraph provides that an attorney may not be detained, searched or taken into custody on circumstances arising from his or her professional activities, except on the basis of a ruling of a county or city court. A law office through which an attorney provides legal services may also not be searched on circumstances arising from his or her professional activities.

As referred in our answers to the previous questionnaire, § 43 of the Bar Association Act also sets forth the following general principles: (i) information disclosed to an attorney is confidential; (ii) media related to the provision of legal services by an attorney are intact; (iii) an attorney is required to maintain the confidentiality of information which has become known to him or her in the provision of legal services, and the confidentiality of persons who request the attorney to provide legal services.

Based on the aforementioned provisions data that has been retained by certain professionals (e.g. lawyers, notaries) may only be used as evidence in certain cases. The evidence gathered using surveillance activities may be used as evidence only if

---

A witness may refuse to give testimony also if the testimony may lay blame on him or her or a person listed above for the commission of a criminal offence or a misdemeanour.
According to § 72, the following persons and their professional support staff have the right to refuse to give testimony as witnesses concerning the circumstances which have become known to them in their professional activities:

1) the ministers of religion of the religious organisations registered in Estonia;
2) counsels and notaries unless otherwise provided by law;
3) health care professionals and pharmacists regarding circumstances concerning the descent, artificial insemination, family or health of a person;
4) persons on whom the obligation to maintain a professional secret has been imposed by law.

If on the basis of a procedural act the court is convinced that the refusal of a person to give testimony is not related to his or her professional activities, the court may require the person to give testimony.

According to § 73 a witness has the right to refuse to give testimony concerning circumstances to which the State Secrets and Classified Information of Foreign States Act applies. If a witness refuses to give testimony in order to protect a state secret or classified information of a foreign state, the investigative body, Prosecutor's Office or court requests the agency in possession of the state secret or classified information of a foreign state to confirm classification of the facts as state secret or classified information of a foreign state. If an agency in possession of a state secret or classified information of a foreign state does not confirm classification of facts as state secret or classified information of a foreign state or does not respond to a request specified above within twenty days, the witness is required to give testimony.

the regulations regarding the authorisation for surveillance activities and the surveillance procedure have been properly followed. In case of any infringement the evidence gathered is not admissible. Furthermore, data regarding the professional activity of the abovementioned professionals may not be used as evidence, except if the professional has already given statements about such data or the data has been published in any manner and all the procedural rules have been followed. Therefore in case of professionals the data is not admissible if the procedural rules are infringed or the data concerns their professional activities and such data has not been published in any manner. According to the amendments entering into force on 1 January 2012, the surveillance activities of professionals may be carried out if the professional has already given statements about such data or the data has been published in any manner or if the authorisation for surveillance of the particular professional has been properly given or it becomes apparent from surveillance of another person that the professional is committing or is about to commit a crime. According to the law in force today, the authorisation (for two months, but may be prolonged) of the preliminary judge or in urgent matters an order of the head of a police authority or the Security Police Board or an official appointed by him or her is required. However, according to the amendments, the authorisation must be given by the preliminary investigation judge for a maximum period of two months which may be prolonged. For example, according to case law from the year 2010 communication between an attorney and his client was deemed admissible evidence because according to the court the data did not concern the provision of legal services.

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?**

   No information available.

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.**

   There are statistics on the amount of inquiries and responses for information by the surveillance and security authorities in 2010. The table shows inquiries concerning the following services: telephone service, mobile phone service, internet connection, e-mail service and internet-telephone service.

	Months 0-3		**Months 3-6**		**Months 6-9**		**Months 9-12**		**Total 2010**	
	Yes	No	Yes	No	Yes	No	Yes	No	**Yes**	**No**
Telephone service	919	471	441	148	347	17306	863	80010	**2570**	**97935**
Mobile phone	191	10	227	7	126	5	112	5	**656**	**27**

service										
Internet connection	322	198	215	90	120	64	156	68	**813**	**420**
E-mail service	28	12	17	6	19	4	11	3	**75**	**25**
Internet phone service	6	1	2	0	0	0	1	0	**9**	**1**
Total	**1466**	**692**	**902**	**251**	**612**	**1737 9**	**1143**	**8008 6**	**4123**	**9840 7**

Yes - means that the inquiry was responded

No - means that it was not possible to respond to the inquiry

Source of information: e-mail of Ms. Anne Tuisk, the chief specialist of communication services of the Technical Surveillance Authority, tel. +372 667 2083, e-mail: anne.tuisk@tja.ee.

B. Country-specific questions

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

Data retention as a whole could be regarded broadly in accordance with the constitution. However, the regime has several shortcomings.

Firstly, it has not been regulated how the retained data may be used in civil litigation (when it may be demanded, how it should be maintained, destroyed, etc.).

Secondly, the methods of secure retention of personal data should be more clearly stated. The proper handling of the retained data may be achieved also through detailed and professional supervision of the communications undertakings, but how the supervision takes place and what are the exact requirements for data retention is not quite clear at the moment.

Finally, as the right to use the retained data by the surveillance and security authority needs proper authorisation (e.g. court order, etc.), there should in principle be no misuse of the retained data. It should be noted however, that the constitutionality of Estonian surveillance laws is under public scrutiny and some legal professionals find that it is too easy to put someone under surveillance.

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?

It is not entirely clear whether the retained data is covered by the secrecy of correspondence. However, it can be inferred from the explanatory memorandum to the amendments of the ECA that introduced the data retention obligations since

2009[2] that data to be retained should not be considered to be covered with secrecy of correspondence. The memorandum states that the restriction of the right to privacy set forth in § 111[1](2) and (3) of the ECA (i.e. clauses regulating data retention) should be differentiated from the restriction of the secrecy of correspondence set forth in § 113 of the ECA (i.e. clause regulating access to communications network). Furthermore, the memorandum explains that from communication perspective, the restriction of the secrecy of correspondence should be considered more severe restraint to fundamental rights than the restriction of the right to private life.

9. Please explain the impact of the proportionality rule when assessing the constitutionality of a measure limiting fundamental freedoms, and what interests have to be balanced within the scope of such assessment.

In Estonia, the Constitutional Review Chamber of the Supreme Court reviews the constitutionality of laws and other legislation of general application. Their judgments mostly use the classic proportionality test, according to which a restriction of freedom must be suitable (proper), necessary and appropriate:

1) Suitable - the restriction is not suitable if it does not promote or help achieve the goal set by the state;

2) Necessary - the restriction is not necessary if there is another less restrictive method to achieve the set goal;

3) Appropriate - the goals of the restriction must be important enough to justify the restriction. More intense the restriction, more essential must be the reasons that justify it. The restricted fundamental freedom must be compared to the principles that are the basis for the restriction and justify it. To determine whether the restriction is appropriate and proportional in the narrow sense different principles should be deliberated.

In case of data retention the principle of privacy and protection of public order need to be assessed and the balance deliberated. In specific cases the courts decide whether there was enough cause to put a person under surveillance based on the information prior to surveillance. The constitutionality of laws regulating surveillance has not been deliberated by the Constitutional Review Chamber of the Supreme Court.

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

According to § 110 of the Code of Criminal Procedure evidence may be collected by surveillance activities in a criminal proceeding if collection of the evidence by other procedural acts is precluded or especially complicated and the object of the

---

[2] Explanatory memorandum to the draft of the Act on the Amendment of Electronic Communications Act and the Public Health Act, available on the website of *Riigikogu*, but only in Estonian: http://www.riigikogu.ee/?page=eelnou&op=ems&emshelp=true&eid=95374&u=20110525152921.

criminal proceeding is a criminal offence in the first degree or an intentionally committed criminal offence in the second degree for which at least up to three years' imprisonment is prescribed as punishment.

A criminal offence in the first degree is an offence where the maximum punishment is imprisonment for a term of more than five years, life imprisonment or compulsory dissolution. First degree criminal offences include robbery, terrorism, manslaughter, murder, criminal organisation, repeated bribery, use of counterfeit money or securities etc.

A criminal offence in the second degree is an offence where the punishment is imprisonment for a term of up to five years or a pecuniary punishment. Second degree criminal offences for which imprisonment at least up to three years is prescribed include negligent homicide, causing serious health damage through negligence, physical abuse, placing in danger, refusal to provide help, unauthorised surveillance, certain sexual offences, certain offences regarding family and children, unlawful handling of narcotic drugs, larceny, acquisition, storage or marketing of property received through commission of criminal offence, certain computer crimes, fraud, unauthorised use of a thing, certain offences against intellectual property, accepting, arranging, granting or giving of bribe or gratuities, failure to report crime, certain offences regarding the environment or economic activities (competition, securities market, taxes, etc.), money laundering, etc.

Additionally, § 110 (1^1) of the Code of Criminal Procedure allows collection of information concerning messages transmitted through commonly used technical communication channels as a single inquiry (i.e. an inquiry concerning a particular telephone call, a particular electronic mail, a particular electronic commentary or another communication session related to the forwarding of a single message) in criminal proceedings concerning the following offences: threatening, infringement of confidentiality of messages, violation of obligation to maintain confidentiality of secrets which have become known in course of professional activities, sexual enticement of children, exhibiting violence to minors, interference in computer data, hindering of operation of computer system, dissemination of spyware, malware or computer viruses, unlawful use of computer system, defamation of official symbols of Republic of Estonia, defamation of official symbols of foreign state or international organisation, defamation or insult of representative of state authority or other person protecting public order, defamation and insulting of court or judge, violation of confidentiality requirement in relation to court proceedings, violation of restriction order, unjustified disclosure and use of business secrets and abuse of inside information.

According to Securities Market Act the Financial Supervision Authority may make an inquiry regarding the retained data in case of a justified suspicion of offences provided in the Securities Market Act. Securities Market Act provides offences regarding misdemeanours in the sphere of securities markets, e.g. violations concerning prospectus, obligations of market participants and issuers, etc.

11. **Does § 111[1] ECA, as a whole, apply exclusively to communications undertakings, as defined by § 2 5) ECA, or to all of the providers mentioned in the corresponding paragraph (e.g., in the case of § 111[1](3) ECA, to *all* internet e-mail service providers and not just to those who, at the same time, also provide publicly available electronic communications services/are considered a 'communications undertaking')?**

    - **If the first: does the reference to the term 'communications undertaking' mean that only providers of electronic communications services are obligated to retain traffic and location data, whereas the operators of public communications network are not obligated by these provisions? What is meant by the term "network service", as mentioned in § 2 6) ECA?**

    - **If the latter: Is it possible to say from the legislative records and/or the political debate whether the legislator was aware of the fact that under the Directive only providers of publicly available electronic communications services and of public communications networks shall be obligated to retain data? If so: is the legislator, according to these or other sources, of the opinion that it is not contrary to EU law to extend the scope of application in this way?**

    Paragraph 111[1](1) of the ECA provides a general data retention obligation only to communications undertakings, who are defined as providers of publicly available electronic communications services in § 2 5) of the ECA. At the same time, § 111[1](3) of the ECA, which sets out the specific obligations, could indeed be interpreted to include a wider range of service providers. It does not appear from the above referred explanatory memorandum that this possible broadening of the scope was intentional.

12. **Please describe the applicable rules on reimbursement of costs in detail. In which form and to which extent (completely, certain percentage of the full costs, lump sum, mere depreciation of book-entry items on tax return) are the costs reimbursed? How and by whom (government authority, provider) are the amounts to be reimbursed calculated? How are the specific data retention costs delimited against the costs for the general storage equipment and the general data storage process?**

    The main rule pursuant to § 111[1](10) of the ECA is that the costs arising from retaining or processing of data is not compensated to the communications undertakings, only the costs regarding the provision of information to surveillance and security authorities are compensated.

    According to § 114 of the ECA, a communications undertaking is compensated for the costs incurred thereby in relation to the provision of the information that has been requested by the surveillance or security authority, in relation to enabling access to the communications network or transmission of messages to the surveillance device of surveillance agencies or security authorities. The costs that are compensated include the cost of hardware and software needed for the transmission of messages to the surveillance device of surveillance agencies or

security authorities, the maintenance costs of these devices, the message transmission costs and the costs of providing the requested information. The value of the hardware and software specified and the cost of maintenance thereof is compensated to the communications undertaking out of the state budget fees sector through the budget of the Ministry of Economic Affairs and Communications. Such fees are paid in instalments over a period of not longer than ten years per each acquired item by way of fixed annual payments to be made once a year. The need to acquire or replace software or hardware, the manner of acquisition, and costs for the acquisition and maintenance must be approved by the Ministry of Economic Affairs and Communications before the acquisition or replacement of the software or hardware. The fees are paid in accordance with the contract entered into between the Ministry of Economic Affairs and Communications and the communications undertaking. The costs related to transmission of messages and provision of information are compensated to the communications undertaking out of the state budget through the budget of the ministry in the area of government to which the surveillance agency or security authority belongs. Such costs are compensated in accordance with the contract entered into between the surveillance agency or security authority and the communications undertaking.

The exact procedures for compensation for the costs are established by the regulation no 160 of 7 July 2005[3] of the Government of the Republic. The costs for electronic connection created in order to provide information and enable access to the communications network are compensated by the surveillance or security authority according to the agreement concluded between the communications undertaking and the surveillance or security authority by fixed monthly payments regardless of the amount of information requests or the amount and type of available data. In the absence of the aforementioned electronic connection, the surveillance or security authority compensates the oral or written requests according to the contract concluded with the communications undertaking. The costs for access to the communications network and transmission of messages are compensated by the surveillance or security authority according to the agreement concluded between the communications undertaking and the surveillance or security authority by fixed monthly payments regardless of the amount of transmitted messages and the extent of the restriction of their privacy rights. If the communications undertaking and the surveillance or security authority do not reach an agreement regarding the compensation of costs, the communications undertaking has no right to refuse from transmission of messages, etc.

13. As regards your answers to questions 38 and 39 of the first questionnaire on the place of data storage: Does Estonian law provide for rules on the transfer of personal data to third countries that correctly transpose the provisions laid down in Chapter IV of Directive 95/46/EC? If so: please provide details of these rules.

These rules are provided in § 18 of the Personal Data Protection Act. Transmission of personal data from Estonia is permitted only to a country which has a sufficient

[3] Available in Estonian at: https://www.riigiteataja.ee/akt/920593

level of data protection. Transmission of personal data is permitted to the Member States of the EU and the States party to the EEA Agreement, and to countries whose level of data protection has been evaluated as sufficient by the European Commission. Transmission of personal data is not permitted to a country whose level of data protection has been evaluated as insufficient by the European Commission.

Personal data may be transmitted to a foreign country which does not meet these conditions only with the permission of the Data Protection Inspectorate if:

1) the data controller guarantees, for that specific event, the protection of the rights and inviolability of the private life of the data subject in such country;

2) sufficient level of data protection is guaranteed in such country for that specific case of data transmission. In evaluating the level of data protection, the circumstances related to the transmission of personal data are taken into account, including the composition of the data, the objectives and duration of processing, the country of destination and final destination of the data, and the law in force in that country.

The Data Protection Inspectorate must inform the European Commission of the grant of such permission.

Additionally, personal data may be transmitted to a foreign country which does not meet the aforementioned conditions without the permission of the Data Protection Inspectorate if:

1) the data subject has granted permission to this effect;

2) the personal data is transmitted in certain cases (in individual cases for the protection of the life, health or freedom of the data subject if it is impossible to obtain the consent of the data subject or if the third person requests information obtained or created in the process of performance of public duties provided by an Act or legislation issued on the basis thereof and the data requested does not contain any sensitive personal data and access to it has not been restricted for any other reasons).

14. In question 40 d) and e) of the first questionnaire, you mention Regulation No. 56 of the Minister of Economic Affairs and Communication of 25 June 2008 "The procedure for retention, passing over to the Technical Surveillance Board, deleting and destroying data, inquiries, log files and applications". Is this Regulation binding on communications undertakings and other bodies concerned? Please describe its content in detail, and, in particular, the measures it provides in the following areas:

- **physical protection of the data retained (e.g. through physically separated storage systems that are disconnected from the internet, located within particularly protected buildings)**
- **secure data storage: cryptographic security (e.g. general obligation to encrypt the data retained, possibly further detailed by specifications e.g. on**

the encryption algorithm to be used or on the safe custody of the crypto-keys)
- **rules on internal access restriction and control (e.g. four-eyes principle, secure authenification mechanisms/certificates)**
- **access logging**
- **secure (irreversible) deletion after expiry**
- **error correction mechanisms (e.g. hash functions, checksums)**
- **secure data transmission (cryptographic security, postal delivery)**
- **access/request procedure (transmission by the provider on request or direct access by the entitled bodies?)**
- **measures to ensure that data transmitted is used exclusively for the designated purpose (e.g. tagging through electronic signature, time-stamp etc)**
- **staff training/internal control mechanisms to ensure compliance with the law and other rules**
- **measures to ensure that the principles of data reduction and data economy are respected (e.g. rules that avoid double retention of data by both the service provider and the operator of the network used for signal conveyance)**

Do the technical and organisational measures described apply specifically and exclusively to the storage and transmission of data in the context of data retention, or to any data processing (in electronic communications) in general? If available, please provide the URL where the Regulation may be accessed (preferably in English).

Regulation No. 56 of the Minister of Economic Affairs and Communication of 25 June 2008 "The procedure for retention, passing over to the Technical Surveillance Board, deleting and destroying data, inquiries, log files and applications" does not provide much more additional information regarding storage of data than the ECA. The regulation applies to storage and transmission of data in the context of data retention pursuant to ECA. This regulation is binding on communications undertakings and other bodies concerned.

According to § 2(2) of the regulation, communications undertakings must designate persons who have access to log files and applications and also register the time when log files and applications were accessed and who accessed it. Further, the provision states that communication undertakings are obliged to retain the data in premises with limited access and surveillance.

Pursuant to § 112(1) and (2) of the ECA, transmission by the provider on request or direct access by the entitled bodies are allowed. For continuous electronic access such an agreement between the communications undertaking and the security and surveillance authority must be concluded. In case of mobile telephone positioning, agreement for continuous electronic access is mandatory.

The regulation is available in Estonian: https://www.riigiteataja.ee/akt/13100712

The general requirements for data storage are provided in the ECA. According to § 111^1(9) of the ECA, upon retaining data, communications undertakings must ensure that:

1) the same quality, security and data protection requirements are met as those applicable to analogous data on the electronic communications network;

2) the data are protected against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

3) appropriate technical and organisational measures are taken to restrict access to the data;

4) no data revealing the content of the communication are retained.

15. Please describe in detail the rules, applicable to data retention, for co-operation among the different bodies accessing the data and between these and other public authorities, as far as they are laid down in the law or otherwise publicly available.

There are no specific publicly available regulations or policies regarding data retention related co-operation between different bodies.

16. Is it legal, under Estonian law, for a competent authority to order that data retained by communications undertakings under the laws transposing the Directive be transferred to a non-EU Member State on the basis of an international co-operation agreement (such as those mentioned in your answer to question 34 of the first questionnaire)? If so: does this require that the relevant data has been requested by an entitled national body for its own purposes before, or is it sufficient for the foreign body to file a corresponding request?

There is no special law or provision regarding such data retention request by foreign authority. As explained in our answer to question 34 of the first questionnaire, any requests by foreign bodies should be sent to the Estonian Ministry of Justice, which is the designated central authority responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. The Estonian Police and Border Control Board is the further point of contact.

17. Please provide information about the independence of the supervisory authorities referred to in your answer to question 35 of the first questionnaire (other than the "Data Protection Inspectorate").

The Prosecutor's Office - as noted in our previous answers, the Prosecutor's Office is a government agency within the administrative area of the Ministry of Justice.

Recent amendments to the Prosecutor's Office Act[4], which were adopted on 16 February 2011 and entered into force on 26 March 2011, introduced a provision, which emphases the independence of the Prosecutor's Office. Paragraph 1(1^1) of the Prosecutor's Office Act stipulates that the Prosecutor's Office is independent upon performance its statutory tasks and its acts on the basis of the Prosecutor's Office Act, other acts and regulations based thereupon.

Security Authorities Surveillance Select Committee of the *Riigikogu* - exercises parliamentary supervision. It is composed of eight members of parliament both from coalition and opposition parties. The committee is a select committee of the *Riigikogu* which exercises supervision over agencies of executive power in questions relating to the activities of security authorities and surveillance agencies, including ensurance of fundamental rights and efficiency of the work of security authorities and surveillance agencies, and in questions relating to supervision exercised thereover. The Prime Minister and the relevant ministers inform the committee of the activities of the security authorities and surveillance agencies and of supervision over their activities and submit an overview of such issues to the committee at least once in every six months. In order to perform its functions, the committee has the right to summon persons and require documents for examination. The committee deliberates drafts of the budget of a security authority concurrently with the deliberation of the draft of the state budget in the *Riigikogu*. The committee submits an overview of the activities of the committee and the results thereof to the *Riigikogu* at least once a year. If an offence is detected, the committee is required to forward the relevant materials to an investigative body or the Chancellor of Justice.

Security Police Board - for comprehensive overview of how the surveillance over Security Police Board is organised, please see http://www.kapo.ee/eng/general-information/supervision/how-supervision-is-organised.

[4] Unofficial English translation of the Prosecutor's Office Act is available at: http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X2050K10&keel=en&pg=1&ptyyp=RT&tyyp=X&query=prokuratuuriseadus.

Update on the Data Retention Regulation in Estonia

Early in year 2011, an act amending the Code of Criminal Proceedings and related acts was passed by the Estonian parliament. The purpose of the amendments was to systemise the regulation pertaining to surveillance activities, set forth specific grounds on which surveillance activities restricting the constitutional rights of persons may be conducted and to provide for a more effective supervision over such activities - and was expected to enter into force on 1 January 2012. However, the passed amendments soon became subject to considerable criticism, which, among others, originated from the Chancellor of Justice and the President of the Republic of Estonia - certain aspects of the amended regulation were said to be in conflict with the Estonian Constitution. This gave rise to a revision of the amendments and ultimately resulted in a new amendment act being passed, which replaced the discussed amendments prior to their entry into force.

The revised amendments entered into force on 1 January 2013. We will hereby highlight the most notable changes as pertains to data retention.

Access to Data Retained by Communications Undertakings

Requesting access to the data the communications undertakings are obligated to retain under § 111^1(2)-(3) of the ECA is not considered a surveillance activity any more. 90^1 of the Code of Criminal Proceedings sets forth that a body conducting proceedings may make enquiries to electronic communications undertakings about the data required for the identification of an end-user related to the identification tokens (e.g. IMEI, IMSI, SIM, IP-address, user name, number, etc.) used in the public electronic communications network, except for the data relating to the fact of transmission of messages.

Any other data as listed under § 111^1(2)-(3) of the ECA (e.g. the date and time of the start and end of the call, the cell ID at the time of commencement of the call, data identifying the geographic location of the base station, in the case of pre-paid anonymous mobile telephone services, the date and time of the initial activation of the service and the cell ID from which the service was activated, the date and time of the log-in and log-off of the Internet access service, the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service) can be requested only with the permission of a Prosecutor's Office in pre-trial procedure and with the permission of a court in court proceedings.

The permission to make inquiries must set out the dates of the period of time about which the requesting of data is permitted. The aforementioned enquiries may be made only if this is unavoidably necessary for the achievement of the objectives of criminal proceedings.

As access to the discussed data is not considered a surveillance activity any more, the list of bodies that may gain access to it has been extended as well. According to § 111^1(11), such bodies are listed as follows: an investigative body, a surveillance agency, the Prosecutor's Office or a court pursuant to the Code of Criminal Procedure; a security

authority; the Data Protection Inspectorate, the Financial Supervision Authority, the Environmental Inspectorate, the Police and Border Guard Board, the Security Police Board and the Tax and Customs Board pursuant to the Code of Misdemeanour Procedure; the Financial Supervision Authority pursuant to the Securities Market Act; a court pursuant to the Code of Civil Procedure; a surveillance agency in the cases provided for in the Organisation of the Defence Forces Act, the Taxation Act, the Police and Border Guard Act, the Weapons Act, the Strategic Goods Act, the Customs Act, the Witness Protection Act, the Security Act, the Imprisonment Act and the Aliens Act.

Grounds for Relying on Surveillance Activities

Before the amendments, the permissibility of relying on surveillance activities in criminal proceedings was, as a rule, tied to the degree of the punishment possible to be imposed for committing a particular offence. As a result of the amendments, this approach was substituted by instead stipulating a list of specific offences in which case surveillance activities can be used (§ 126^2(2) of the Code of Criminal Procedure). Also, the types of persons in respect of whom surveillance activities may be conducted has been laid down by the law (§ 126^2(3)-(4) of the Code of Criminal Procedure).

Permission for Conducting Surveillance Activities

Before the amendments, it was possible to conduct certain surveillance activities without the prior permission by the preliminary investigation judge in cases of urgency, i.e. only on the basis of an according ruling by the director of the relevant surveillance agency, which needed retroactive approval from the preliminary investigation judge at first possibility. Such exceptions have now been abolished and conducting surveillance activities can only be permitted on grounds of permission by the Prosecutor's Office or the preliminary investigation judge - even in cases of urgency.

***

As mentioned above, this overview constitutes our selection of the most notable changes to Estonian regulation pertaining to data retention by communications undertakings. The procedure of surveillance activities stipulated in the Code of Criminal Procedure has also undergone many changes that are considerably more detailed and many of them not as significant. As such changes are currently not reflected herein, please let us know if you would need us to provide you a more detailed analysis.

Please also find links to unofficial translations of the relevant legislation:

Code of Criminal Procedure:
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X60027K9&keel=en&pg=1&ptyyp=RT&tyyp=X&query=kriminaalmenetluse+seadustik

Electronic Communications Act:
http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X90001K7&keel=en&pg=1&ptyyp=RT&tyyp=X&query=elektroonilise+side+seadus