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

Finland

Anne Yliniva-Hoffmann

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

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

I. Legal provisions

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

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

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

Yes.

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

2. What are the reasons for the transposition not (or only in parts) to have been effected (e.g. (purely) formal delays in the legislative procedure, constitutional

law concerns, legal policy issues, socio-ethical concerns, incompatibility with the national legal system etc)?

Not applicable.

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

   Not applicable.

4. **In case draft legal acts are existent, or a law that had already been enacted/come into force has subsequently been abrogated by a court decision or for other reasons: Please describe the content of the provisions on the basis of questions 5, and 7 to 35.**

   Not applicable.

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

General questions

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

   Yes (Act on the Protection of Privacy in Electronic Communications). However, the translation is unofficial:
   http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf

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

   The relevant regulations have been in force since 1 June 2008.

   Finland had in accordance with Article 15(3) of the Directive declared that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail to 15 March 2009 (see also Chapter 11 Sec. 44 of the Act 516/2004). (the Directive: Declaration by Finland)

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

According to Chapter 1 Sec. 10 (The Right to Privacy) of the Constitution of Finland[1] provisions on the protection of personal data are laid down by an Act.

In the present case transposition has been achieved through an Act of Parliament (Finnish Act on the Protection of Privacy in Electronic Communications 16.6.2004/516 (hereinafter referred to as the "Act")). The Act has been amended through a Government Bill (HE 158/2007; which became the Act 343/2008 on the Amendment of Act on the Protection of Privacy in Electronic Communications[2]) to meet the requirements of the Directive. After this, the Act has partly been amended several times (19.12.2008/865, 13.3.2009/125, 11.9.2009/686 and 22.5.2011/365).

According to several statements[3] of the Parliamentary Constitutional Commitee and Administration Commitee at least the following subject-matters shall be ruled by Act:

- the objective of the registration,
- the content of the personal data registered,
- the permitted use of the data,
- the transferability of data,
- the provision of data via technical connection,
- the duration of the data storage in the register and
- the legal protection of the person registered.

Certain specifying and complementary rules, e.g. concerning the concrete information content of a register, may be issued by Decree.

The internet pages of the Finnish Ombudsman for Data Protection (http://www.tietosuoja.fi/).), as well as those of the Finnish Ministry of Transport and Communications (http://www.lvm.fi/web/fi/etusivu) and the Finnish Communications Regulatory Authority (hereinafter referred to as FICORA http://www.ficora.fi) provide further information on the topic in question. These pages also contain general information on data security in matters relating to electronic communication.

---

1 The Constitution of Finland 731/1999 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf; and in German at: http://www.finlex.fi/fi/laki/kaannokset/1999/de19990731.pdf (both translations are unofficial).

2 The Government Bill HE 158/2007 is available at: http://www.finlex.fi/fi/esitykset/he/2007/20070158; Act 343/2008 is available at: http://www.finlex.fi/fi/laki/alkup/2008/20080343 (both only in Finnish).

3 These are inter alia PeVL 14/1998 vp, PeVL 12/2002 vp, HaVL 16 and 19/1998 vp, HaVM 25 and 26/1998 vp.

A Government Decree concerning the obligation of identification data retention is under discussion at the moment (LVM016:00/2011). The purpose of the decree is to ensure that the practice of implementing as well as the requirements and obligations set for the data retention are unambiguous for the common system a third party offers to the telecommunications operators. The decree is included to a project led by the Ministry of Transport and Communication, which additionally aims to amend the Sec. 14a-c of the Act in order to extend the use of data from investigating, solving and considering charges to uncovering and preventing criminal acts. The project started on 29th October 2009 and is currently circulated for comments.

FICORA provides a regulation concerning the obligation of identification data retention (53/2008 M) in accordance with the Sec. 14a of the Act; a regulation concerning the maintenance of information security (47 C/2009 M) in accordance with the Sec. 19 and 20 of the Act; and a recommendation on processing the identification data retention (308/2004 S) in accordance with the Sec. 15 of the Act. The documents are provided only in Finnish.

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

Yes.

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

Only partially. Chapter 1 Sec. 2 (1)-(18) of the Act includes the relevant definitions. The term "user" is defined correspondingly in the Act. The term "data" is defined through two different terms: *identification data* and *location data*. The term "telephone service" corresponds to the terms *communication service* and *network service* used in the Act. The terms "userlD", "cellID" and "unsuccessful call attempt" are not defined in the Act. The definition of the term "processing" corresponds to the term "processing of personal data" of Directive 95/46/EC. The term "subscriber" corresponds to the term subscriber of Directive 2002/21/EC. The term "value added service" corresponds to the term value added service of Directive 2002/58/EC. The following terms are defined in the Act, but not in any of the abovementioned Directives: *message, public communications network, telecommunications operator, corporate or association subscriber, information security, service operator, Internet phone service, targeted emergency message, other targeted message from the authorities, targeted message from the authorities* and *telecommunications contractor.*

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?

Identification data and location data have to be retained.

All messages, identification data and location data are confidential unless the Act or another Act provides otherwise. Current and former employees of a telecommunications operator, value added service provider, corporate or association subscriber or telecommunications contractor shall not disclose knowledge obtained through their employment about messages, identification data or location data without the consent of a party to the communication or the party to whom the location data applies, unless otherwise provided by law.

Telecommunications operators, value added service providers and corporate or association subscribers and any persons acting on their behalf may process location data for the purpose of providing and using value added services. However, the provisions do not, unless otherwise provided by law, apply to location data rendered such that it cannot, in itself or in combination with other data, be associated with a specific subscriber or user. Processing of data is allowed only to the extent required for the purpose of the processing, and it shall not limit the protection of privacy any more than is necessary. After processing, the location data shall, unless otherwise provided by law, be destroyed or rendered such that it cannot be associated with a specific subscriber or user.

A service operator obliged to submit a telecommunications notification shall ensure, under the conditions prescribed below, that data referred to in Article 5 of the Directive 2006/24/EC are retained for a period of 12 months from the date of the communication (Chapter 3 Sec. 14a of the Act). Such data may be used only for the purposes of investigating, solving and considering charges for criminal acts referred to in chapter 5 a(3)(1) of the Coercive Measures Act (450/1987). The retention obligation applies to data related to a service operator's telephone service or additional service through a fixed network, telephone service, additional service, SMS service, EMS service or multimedia service through a mobile network, Internet connection service provided by a service operator, e-mail service provided by a service operator, Internet telephony service provided by a service operator, a call for which a connection has been established but the call remains unanswered or is prevented from being connected due to network management measures.

Therefore, the Finnish Act on the Protection of Privacy in Electronic Communications goes beyond the obligations mentioned in the Directive, thus it is more exhaustive than the Directive.

Data on unsuccessful call attempts do have to be retained, (Chapter 3 Sec. 14a of the Act).

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.

Billing-related data must be stored for a minimum of three months from the due date of the bill or the saving of the identification data, whichever is later. Such data must not, however, be stored beyond the time the debt becomes statute-barred under the Act on statute-barred debt (728/2003). However, in the case of a dispute over a bill, the data pertaining to that bill must be stored until the matter has been settled or resolved.

According to the above-mentioned act, the retention obligation applies to data related to: a service operator's telephone service or additional service through a fixed network, telephone service, additional service, SMS service, EMS service or multimedia service through a mobile network, Internet connection service provided by a service operator, e-mail service provided by a service operator, Internet telephony service provided by a service operator, a call for which a connection has been established but the call remains unanswered or is prevented from being connected due to network management measures. The retention obligation does not apply to the contents of a message or identification data generated through the browsing of websites.

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

For the purposes of the authorities, for the purposes of a corporate or association subscriber’s right to store identification data in cases of misuse, for the purposes of a corporate or association subscriber’s right to process data for investigating disclosures of business secrets, for the purposes of a corporate or association subscriber’s right to process data for investigating unauthorized use of information society service, communications network or communications service, as well as for the purposes of a telecommunications operator’s and value added service provider’s right to process data in cases of misuse.

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)?

According to the Finnish Act on the Protection of Privacy in Working Life 759/2004[4], the employer is only allowed to process personal data directly necessary for the employee's employment relationship which is connected with managing the rights and obligations of the parties to the relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned. No exceptions can be made to the necessity requirement, even with the employee's consent.

According to the Finnish Act on Health Care Professionals 559/1994[5], no health care professional may reveal without permission to a third party any secret concerning an individual or a family that he or she has learned on the basis of his or her position or tasks. The obligation to maintain secrecy shall continue after their professional activity has ended.

According to the Finnish Act on the Status and Rights of Patients 785/1992[6], health care professionals or other persons working in a health care unit or carrying out its tasks shall not give information contained by patient documents to outsiders without a written consent by the patient. If a patient is not capable of assessing the significance of the consent, information may be given by his/her legal representative's written consent. In this Act outsiders refer to persons other than those who participate in the care of the patient or in carrying out jobs related to it in the health care unit in question or by its order. The secrecy obligation remains in force after termination of the employment relationship or the job. However, there are a few exceptions to this main rule.

Also according to the Finnish Personal Data Act 523/1999[7], processing of sensitive data is prohibited. Personal data are deemed to be sensitive, if they relate to or are intended to relate to race or ethnic origin, the social, political or religious affiliation or trade-union membership of a person, a criminal act, punishment or other criminal

---

4 The Act on the Protection of Privacy in Working Life 759/2004 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/2004/en20040759.pdf

5 The Act on Health Care Professionals 559/1994 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1994/en19940559.pdf

6 The Act on the Status and Rights of Patients 785/1992 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1992/en19920785.pdf

7 The Personal Data Act 523/1999 ist available in English at:http://www.finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf

sanction, the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person, the sexual preferences or sex life of a person, or the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person. However, there are several exceptions to this main rule[8].

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.

Billing-related data must be stored for a minimum of three months from the due date of the bill or the saving of the identification data, whichever is later. Such data must not, however, be stored beyond the time the debt becomes statute-barred under the Act on Statute-barred Debt. However, in the case of a dispute over a bill, the data pertaining to that bill must be stored until the matter has been settled or resolved.

A corporate or association subscriber shall draw up a report of manual processing of identification data showing the grounds for the processing, and the time and duration of the processing, the reason for using manual processing of identification data, names of the processors involved or the name of the person who has made the processing decision. People involved in the processing shall sign the report. The report shall be kept for at least two years from the end of the processing.

A service operator obliged to submit a telecommunications notification shall ensure that data referred to in Article 5 of the Directive 2006/24/EC are retained for a period of 12 months from the date of the communication. Such data may be used only for the purposes of investigating, solving and considering charges for criminal acts referred to in chapter 5 a(3)(1) of the Coercive Measures Act.

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 Ministry of Transport and Communications, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman are entitled to access information necessary for the carrying out of their duties from any telecommunications operator, value added service provider, corporate or association subscriber, telecommunications contractor, service provider processing data describing the use of its service, direct marketing party, subscriber directory service

---

[8] These exceptions are scattered into different acts and no exhaustive list exists. However, as an example, according to the Finnish Personal Data Act Sec. 12, the abovementioned list of prohibitions does not prevent processing of data necessary for drafting or filing a lawsuit or for responding to or deciding of such a lawsuit *or* a health care unit or a health care professional from processing data collected in the course of their operations and relating to the state of health, illness or handicap of the data subject or the treatment or other measures directed at the data subject, or other data which are indispensable in the treatment of the data subject. An unofficial translation of the Finnish Personal Data Act can be found at http://www.tietosuoja.fi/uploads/hopxtvf.HTM.

or directory inquiry service provider, or anyone acting on their behalf, concerning their activities. However, the right of access to information granted to the Ministry of Transport and Communications, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman does not apply to information on confidential messages, identification data or location data.

A telecommunications operator is obliged to disclose the following to an Emergency Response Centre, a Marine Rescue Coordination Centre, a Marine Rescue Sub-Centre or the Police for processing purposes: identification data and location data of the subscriber connection and terminal device from which an emergency call is placed, and information on the subscriber, user and installation address, and identification data and location data showing the location of the user terminal device and subscriber connection to which the emergency call applies if, in the considered opinion of the authority receiving the emergency call, the user is in obvious distress or immediate danger.

The right of authorities to receive identification data for the purpose of preventing, uncovering or investigating crimes has to be grated by an act. As the power of relevant authorities to access such data is scattered into different acts, it is difficult to provide with an exhaustive answer. However, such provisions can be found at least from the following Acts;

1) According to the Finnish Police Act[9] Sec. 35, a member of the senior policemen is entitled to decide upon the request to receive confidential data.

2) According to the Finnish Act on the Processing of Personal Data by the Border Guard (579/2005) Sec. 17, an officer with the power of arrest is entitled to decide upon obtaining confidential data.

3) According to the Finnish Customs Act (1466/1994) Sec. 28, customs authority is entitled to obtain confidential data. According to the Sec. 4 of the same Act, the competent authority and the customs authority referred to in the Community Customs legislation is the National Board of Customs unless another Act provides otherwise.

4) According to the Finnish Coercive Measures Act Sec. 5, a competent court shall decide upon grating a permit from a written request from an officer with the power of arrest, e.g. for obtaining the location data of a mobile communications device.

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

[9] The Police Act 493/1995 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1995/en19950493.pdf

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)?

According to the Act, processing is only allowed to the extent necessary for the purpose of such processing, and it may not limit the confidentiality of messages or the protection of privacy any more than is necessary. Identification data may only be disclosed to those parties entitled to process it in the given situation. After processing, messages and identification data must be destroyed or rendered such that they cannot be associated with the subscriber or user involved, unless otherwise provided by law.

According to the Personal Data Act, personal data must not be used or otherwise processed in a manner incompatible with such purposes. Later processing for purposes of historical, scientific or statistical research is not deemed incompatible with the original purposes. It must be appropriate and justified to process personal data in the operations of the controller. The purpose of the processing of personal data, the regular sources of personal data and the regular recipients of recorded personal data shall be defined before the collection of the personal data intended to be recorded in the file or their organisation into a personal data file. The purpose of the processing shall be defined so that those operations of the controller in which the personal data are being processed are made clear.

According to the Act on the Processing of Personal Data by the Police 761/2003[10], the data referred to in the Personal Data Act may be collected and recorded in a police personal data file and otherwise processed if the data is *necessary for the purpose of use of the file*. The data referred to in the Personal Data Act may only be collected and recorded in a police personal data file or otherwise processed if this is *essential for the performance of an individual police duty*. The data may also be collected and recorded in a police personal data file and otherwise processed if this is *essential to ensure the personal safety of the data subject or the occupational safety of the police*.

According to the Act on the Status and Rights of Patients, information included in patient documents may be given if there are express provisions on giving it or on the right of access to it in the law, information necessary for the arranging of examination and treatment of the patient may be given to another health care unit or health care professional, and a summary of the treatment provided may be given to the health care unit or the health care professional that referred the patient for treatment and to a physician possibly appointed to be responsible for the care of the patient in accordance with the patient's or his/her legal representative's orally given consent or consent that is otherwise obvious from the context, information necessary for arranging and providing the examination and care of a patient may be given to another Finnish or foreign health care unit or health care professional, if the patient, owing to mental health disturbance, mental handicap or for comparable reason is not

[10] The Act on the Processing of Personal Data by the Police 761/2003 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/2003/en20030761.pdf

capable of assessing the significance of the consent and he/she has no legal representative, or if the patient cannot give the consent because of unconsciousness or for comparable reason, information about the identity and state of health of a patient may be given to a family member of the patient or to other person close to the patient, if the patient is receiving treatment because of unconsciousness or for other comparable reason, unless there is reason to believe that the patient would forbid this, and information on the health and medical care of a deceased person provided when the person was still living may be given upon a justified written application to anyone who needs the information in order to find out his/her vital interests or rights, to the extent the information is necessary for that purpose; the acquiring party may not use or forward the information for some other purpose.

What is provided in the Act on the Openness of Government Activities 621/1999[11], the Act on National Personal Data Registers for Health Care 556/1989 and in the Personal Data Act shall apply to the supplying of information contained in patient documents for scientific research and compilation of statistics. Furthermore, the Ministry of Social Affairs and Health may, in individual cases, for purposes of scientific research grant permission to obtain information from such patient documents of a unit providing health care services referred to in the Act on Private Health Care 152/1990 and of self-employed health care professionals that cannot be regarded as authorities' documents referred to in the Act on the Openness of Government Activities. The permission may be granted if it is obvious that the giving of the information does not violate the interests for the protection of which the secrecy obligation has been prescribed. When considering the granting of permission it must been taken care that the freedom of scientific research is secured. The permission can be issued for a fixed period of time, and necessary regulations for the protection of private interests must be appended to it. The permission can be cancelled if considered justified.

The Act on the Processing of Personal Data in connection with the Enforcement of Punishment 422/2002 provides a number of grounds for the processing of personal data as well.

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

According to the Act on the Processing of Personal Data by the Police, the data referred to in the Personal Data Act may only be collected and recorded in a police personal data file or otherwise processed if this is **essential for the performance of an individual police duty**. The data may also be collected and recorded in a police personal data file and otherwise processed if this is **essential to ensure the personal safety of the data subject or the occupational safety of the police**.

[11] The Act on the Openness of Government Activities 621/1999 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990621.pdf and in German at: http://www.finlex.fi/fi/laki/kaannokset/1999/de19990621.pdf

The Police Act states that the police have the right, notwithstanding the secrecy obligation, to obtain free of charge from an authority or a body assigned to perform a public function any information and documents **necessary to carry out an official duty** unless disclosing such information or documents to the police or using information as evidence is prohibited or restricted by law. When assessing the continued validity of a driving license, firearm permit or other such license, the police have the right, on making a justified request, to obtain information on the license holder's state of health, use of intoxicants or violent behavior, notwithstanding the secrecy obligation, if there are reasons to suspect that the license holder **no longer meets the conditions set for obtaining** a license. At the request of a commanding police officer, the police have the right to obtain any information **necessary to prevent or investigate an offence**, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members or employees of an organization. The police have the same right to obtain information needed in a police investigation if **an important public or private interest so requires**.

For further information, please see answers to questions 14 and 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?

The main rule is that no court order has to be obtained. However, no Act provides an exhaustive list of exceptions for this main rule.

To provide the question with an example, according to the Police Act, the court shall decide on telecommunications interception, telecommunications monitoring, gathering information on the location of mobile stations and technical surveillance in cases in which the interception or technical observation requires the placing of the device used for surveillance in a room or premises in which the person to be put under surveillance is staying, or inside a vehicle used by the person to be put under surveillance or in which a person in the custody of the Finnish Prison Service is subjected to interception or technical observation. The matter shall be decided without consulting the person to be put under surveillance or the occupant of the premises to be intercepted or observed.

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?

According to the Personal Data Act the controller shall, when collecting personal data, see to that the data subject can[12] have information on the controller and, where

---

[12] The Finnish Personal Data Act Sec. 24 precisely provides that the data subject *can* have information --. And as mentioned above, *this information shall be provided at the time of collecting and recording of the data or, if the data are obtained from elsewhere than the data subject and intended*

necessary, the representative of the controller, on the purpose of the processing of the personal data, on the regular destinations of disclosed data, as well as on how to proceed in order to make use of the rights of the data subject in respect to the processing operation in question. This information shall be provided at the time of collection and recording of the data or, if the data are obtained from elsewhere than the data subject and intended for disclosure, at the latest at the time of first disclosure of the data.

The duty of providing information may be derogated from, if the data subject already has the relevant information, if this is necessary for the protection of national security, defence or public order or security, for the prevention or investigation of crime or for carrying out the monitoring function pertaining to taxation or the public finances, or where the data are collected from elsewhere than the data subject, if the provision of the information to the data subject is impossible or unreasonably difficult, or if it significantly damages or inconveniences the data subject or the purpose of the processing of the data and the data are not used when making decisions relating to the data subject, or if there are specific provisions in an Act on the collection, recording or disclosure of the data.

Relating to processing for marketing purposes, telecommunications operators shall, prior to obtaining consent, inform subscribers or users about what identification data is to be processed and how long the processing will last. When it comes to processing for the purposes of technical development the subscribers or users shall, prior to the start of the processing, be informed of what identification data is to be processed and how long the processing will last. The information may be given only once.

A controller shall provide the data subject with the data contained in the credit data file and pertaining to the data subject, as well as with the information on the controller and certain processing, at the time when the first entry on the data subject has been recorded into the file. Anyone who has obtained personal credit data on the data subject for the purpose of making a decision pertaining to the data subject shall notify the data subject of the use of the credit data in the decision-making, of the file from which the data have been obtained, of the time when the data have been obtained, if the rejection of credit or another decision negative from the point of view of the data subject is based on the credit data. Where the name and contact information of an individual have been obtained from a personal data file for the

---

for disclosure, at the latest at the time of first disclosure of the data. As regard to the Government Bill 96/1998, the purpose of this section was to create an *obligation* for the controller to ensure, when collecting the data, that the data subject can have all relevant information about collecting and processing data, and about the requirements set for the exceptions. The principle of good registration practice may as well require that the data subject shall be informed about the processing. In addition, according to the Sec. 10 of the Finnish Personal Data Act, the data subject can have information about the processing of his personal data from a file description which contains the same information as provided by the Sec. 24 of the same Act (one example on how to see to the obligation). According to the Sec. 30 of the same Act, the data subject has the right to prohibit the collector to process the information concerning him with regard to direct mail advertising, distance sale or any other direct marketing, market or opinion survey, person register or genealogy.

purposes of direct marketing, distance selling or other direct advertising, or of market research or an opinion poll, or for a comparable addressed delivery, the file used, the controller and the address of the controller shall be mentioned. A teleseller shall give the same information upon request.

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 above.

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?

According to the Act, an appeal may be made in compliance with the provisions of the Finnish Administrative Judicial Procedure Act 586/1996[13] against decisions of the Finnish Communications Regulatory Authority or the Data Protection Ombudsman taken under this Act. In their decisions, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman may order that the decision be complied with before it has gained legal force. However, the appellate authority may prohibit enforcement until the appeal has been resolved. Whoever wilfully violates the obligations provided by the Sec. 42 of the Act[14] shall be imposed a fine for a violation of protection of privacy in electronic communications, unless a more severe penalty is provided elsewhere.

The Personal Data Act states that the decisions of the Data Protection Ombudsman and the Data Protection Board are subject to appeal in accordance with the provisions of the Finnish Administrative Judicial Procedure Act. The Data

---

13 The Administrative Judicial Procedure Act 586/1996 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1996/en19960586.pdf

14 Sec. 42(2) of the Act provides the following: "Whoever wilfully 1) violates the prohibition on the possession, importing, manufacture or distribution of any system or part of a system for decoding the technical protection of electronic communications provided in section 6(2); 2) neglects the duties provided in section 7; 3) neglects the duties provided in section 19 regarding the information security of his or her services or of the processing of identification data and location data; 4) neglects the notification requirement provided in section 21(2) or section 35(4); 5) processes identification data or location data in violation of what is provided in Chapters 3 and 4; 6) neglects to comply with the provisions of section 24 regarding call itemization of bills; 7) neglects to comply with the provisions of section 25 regarding the processing of personal data contained in telephone directories and other subscriber directories, the notifying of subscribers regarding the purpose and use of such directories, the removing and rectifying of information, the right to prohibit use or the rights of legal persons; or 8) practices direct marketing in violation of provisions in Chapter 7; or 9) neglects to comply with the provisions of 13g–13i regarding drawing up and issuing a report or a prior notification to the user, the employees' representative or the Data Protection Ombudsman shall be imposed a fine for a *violation of protection of privacy in electronic communications*, unless a more severe penalty is provided elsewhere."

Protection Ombudsman may appeal against the decision of the Data Protection Board.

The Data Protection Ombudsman may impose a threat of a fine, in accordance with the Finnish Act on Threats of a Fine 1113/1990, in order to reinforce the duty to provide access to data, the Data Protection Board may do likewise in relation to the duty to provide access to data. The controller is liable to compensate for the economic and other loss suffered by the data subject or another person because of processing of personal data in violation of the provisions of this act. A person who intentionally or grossly negligently and contrary to the provisions in this act violates it, thus compromising the protection of the privacy of the data subject or his/her rights, shall be sentenced for a personal data violation to a fine, provided that a more severe penalty is not provided in another act[15].

21. Are there any legal provisions protecting the data retained against unauthorised access in a particular way (not: purely technical guidelines or organisational measures, see question 40 d) in this regard)? Please describe the content of these provisions.

Yes, although indirectly. The Act states that a telecommunications operator subject to notification or licence shall pay an annual information security fee to the Finnish Communications Regulatory Authority. The information security fee covers the costs incurred by the Finnish Communications Regulatory Authority for carrying out the duties provided in this Act concerning telecommunications operators.

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

After processing messages and identification data they must be destroyed or rendered in a way that they cannot be associated with the subscriber or user involved, unless otherwise provided by law.

A service operator obliged to submit a telecommunications notification shall ensure that data referred to in Article 5 of the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC are retained for a period of 12 months[16] from the date of the communication. Such

---

15 Sec. 42(1) of the Act refers to the Finnish Penal Code, which provides the more specific regulations and penalties concerning communications secrecy violation, unauthorised access to data, breach of the obligation of secrecy and breach of confidentiality.

16 The Act does not provide a direct time limit for the bodies accessing data to destroy or render confidential messages, identification data and location data (see Sec. 8(3) and 16), as it only states the obligation to commence "after processing"). Whereas according to the Sec. 33(5), The Finnish Communications Regulatory Authority and the Data Protection Ombudsman shall destroy any information on confidential messages, identification data and location data received when this information is no longer necessary for carrying out the duties or the processing of any criminal case concerning the information. Information on confidential messages, identification data and location data shall be destroyed no later than two years, or ten years in the case of information pertaining to

data may be used only for the purposes of investigating, solving and considering charges for criminal acts referred to in the Finnish Coercive Measures Act.

According to the Personal Data Act, a personal data file shall, when it is no longer necessary for the operations of the controller, be destroyed, unless specific provisions have been issued by an Act or by lower-level regulation on the continued storage of the data contained therein or the file is transferred to be archived.

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.

According to the Act, telecommunications operators are obligated to retain the data. A telecommunications operator is defined as a network operator or service operator. Only a service operator obliged to submit a telecommunications notification is obliged to retain the data.

When service operators are retaining the data, they should do it in a manner which is to avoid overlapping activity. According to the Government Bill 158/2007, the purpose of this principle is to prevent service operators from acting independently according to their retention obligations and causing unreasonable costs by invoicing afterwards the authorities responsible for covering the retention expenses. Additionally, the data has to meet the necessity of such retention and the service operator with the actual retention obligation has to be found among the others. Thus, it is a question of avoiding unreasonable expenses, retaining only necessary data and securing the data retention in practice.

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?

Private persons and civic organisations, as well as corporate or association subscribers, are exempt from the obligation to retain data.

The *notification obligation* does not apply to general telecommunication provided that it is temporary and directed towards a small amount of recipients, or is otherwise of minor significance.

---

an investigation of a violation of information security, from the end of the calendar year during which the information was received or a decision or sentence in the matters referred to in this subsection entered into legal force. However, the regulation concerning the destruction of the abovementioned data may be specified by other Acts. As an example, according to the Chapter 4 of the Act on the Processing of Personal Data by the Border Guard, destroying the data is generally depending on the limited amount of years, unless the information is no longer necessary for carrying out the duties. This necessity must be controlled within certain periods.

The Government Bill on the Communications Market Act (112/2002) defines "telecommunications provider", and provides some examples as follows: firstly, general telecommunications can be considered as temporary when it has an experimental character (e.g. an institute of higher education provides this function as a teaching method; temporality shall be estimated case by case); secondly, telecommunications at a network consisting under 500 subscribers can be considered as an example of the small amount of recipients; and thirdly, a general telecommunications at the maritime mobile network can be considered as an example of the minor significance.

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

The following categories have been retained before the Directive entered into force: billing-related data, reports by a corporate or association subscriber and detailed event log information on any processing of identification data.

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 Act also states that telecommunications operators and value added service providers shall maintain the information security of their services. Corporate or association subscribers shall maintain information security in processing their users' identification data and location data. Maintaining information security in such services or processing means taking measures to ensure operating security, communications security, hardware and software security and data security. These measures shall be commensurate with the seriousness of threats, level of technical development and costs. If a specific threat is posed to the information security of a service, the telecommunications operator and value added service provider shall immediately notify the subscriber of the threat and inform him or her of the measures available to subscribers and users for combating the threat, and the probable costs of such measures.

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

The investments fees originating from the implementation of the national law are according to the Finnish Communications Regulatory Authority estimated to EUR 5—8 million, when the data is retained for twelve (12) months. The yearly running costs would be considerably smaller than this, estimated to be less than ten (10) per cent of the investment fees.

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?

Yes, the parties do receive reimbursement.

According to the Finnish Communications Market Act 393/2003[17], a telecommunications operator's right to receive a compensation from state funds applies only to the direct costs of the investment, use and maintenance of systems, equipment and software acquired to meet the needs notified by a public authority. The telecommunications operator's right to receive compensation from state funds also covers the direct costs incurred from any measures ordered by a public authority. Decisions on the compensation for costs incurred are made by the Finnish Communications Regulatory Authority.

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

Chapter 9 of the Act, regulating the guidance and supervision authorities' right to access information, disclosure of information held by the supervision authorities, disclosing information to emergency services authorities, the obligation of a telecommunications operator to transmit a targeted message from the authorities, certain other authorities' right of access to information, as well as the user's special right of access to information.

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.

According to the Act, whoever wilfully violates the prohibition on the possession, importing, manufacture or distribution of any system or part of a system for decoding the technical protection of electronic communications, neglects the duties provided in section 7, neglects the duties regarding the information security of his or her services or of the processing of identification data and location data, neglects the notification requirement, processes identification data or location data in violation of what is provided in Chapters 3 and 4, neglects to comply with the provisions regarding call itemisation of bills, neglects to comply with the provisions regarding the processing of personal data contained in telephone directories and other subscriber directories, the notifying of subscribers regarding the purpose and use of such directories, the removing and rectifying of information, the right to prohibit use or the rights of legal persons; or practices direct marketing in violation of provisions in Chapter 7, or neglects to comply with the provisions regarding drawing up and

[17] The Finnish Communications Market Act 393/2003 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/2003/en20030393.pdf

issuing a report or a prior notification to the user, the employees' representative or the Data Protection Ombudsman, shall be imposed a fine for a violation of protection of privacy in electronic communications, unless a more severe penalty is provided elsewhere. If the offence is deemed petty, sentence shall not be passed.

In the Act reference is made to the Finnish Criminal Code 39/1889[18] (Chapter 38), which is applicable as follows:

A person who in violation of a secrecy duty provided by an Act or Decree or specifically ordered by an authority pursuant to an act discloses information which should be kept secret and which he or she has learnt by virtue of his or her position or task or in the performance of a duty, or makes use of such a secret for the gain of himself or herself or another shall be sentenced for a secrecy offence to a fine or to imprisonment for a maximum of one year.

If the secrecy offence, in view of the significance of the act as concerns the protection of privacy or confidentiality, or the other relevant circumstances, is petty when assessed as a whole, the offender shall be sentenced for a secrecy violation to a fine. Also a person who has violated a secrecy duty referred to in section 1 and it is specifically provided that such violation is punishable as a secrecy violation, shall also be sentenced for a secrecy violation.

A person who unlawfully opens a letter or another closed communication addressed to another or hacks into the contents of an electronic or other technically recorded message which is protected from outsiders, or obtains information on the contents of a telephone call, telegram, transmission of text, images or data, or another comparable telemessage transmitted by telecommunications or on the transmission or reception of such a message shall be sentenced for message interception to a fine or to imprisonment for a maximum of one year. An attempt is punishable.

If in the message interception the offender commits the offence by making use of his or her position in the service of a telecommunications company, as referred to in the Act on the Protection of Electronic Messages or his or her other special position of trust, the offender commits the offence by making use of a computer program or special technical device designed or altered for such purpose, or otherwise especially methodically, or the message that is the object of the offence has an especially confidential content or the act constitutes a grave violation of the protection of privacy and the message interception is aggravated also when assessed as a whole, the offender shall be sentenced for aggravated message interception to imprisonment for a maximum of one year. An attempt is punishable.

A person who by using an access code that does not belong to him or her or by otherwise breaking a protection unlawfully hacks into a computer system where data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a

[18] The Criminal Code 39/1889 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf

computer break-in to a fine or to imprisonment for at most one year. Also a person who, without hacking into the computer system or a part thereof, by using a special technical device unlawfully obtains information contained in a computer system, shall be sentenced for a computer break-in. An attempt is punishable.

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?

General guidance and development for the purpose of implementing this Act is the responsibility of the Ministry of Transport and Communications. The Finnish Communications Regulatory Authority and the Data Protection Ombudsman serve as supervisors.

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?

A service operator under the retention obligation shall discuss the implementation and application of data retention with the Ministry of the Interior in order to ensure that all data considered necessary by the authorities will be retained. If no consensus is reached on the implementation of data retention, the service operator decides on the technical implementation of the retention. The implementation shall follow the principles of cost-efficiency and consider the business needs of the service operator, the technical features of the systems, and the needs of the authority paying for the costs for the retention. Data should be retained in such a way as to avoid the same data being retained by several service operators. It must be ensured that the data retained can be transmitted to the authorities entitled to it without undue delay. A service operator under the retention obligation shall, together with a network operator if necessary, ensure that the obligation is met in such a way that the available data processed by the network operator in providing the service operator's service shall be retained. A service operator under the retention obligation shall ensure that information about data retention and its purposes is available to the subscriber.

34. On what legal basis does the exchange of retained data with other EU Member States, other EEA Member States and (if permitted) third countries (e.g. CoE Member States party to the Cybercrime Convention) take place? Do foreign

state bodies avail of a right (vis-à-vis the obligated party) to access the retained data directly? If the answer is negative: Which (national) authorities are responsible for cross-border data exchange (the conveyance of outgoing requests and the processing of (responses to) incoming requests)?

According to the Personal Data Act, personal data may be transferred to outside the European Union or the European Economic Area only if the country in question guarantees an adequate level of data protection. The adequacy of the level of data protection shall be evaluated in the light of the nature of the data, the purpose and duration of the intended processing, the country of origin and the country of final destination, as well as the general and sectoral legal provisions, codes of conduct and security measures applied in that country.

No.

The Data Protection Ombudsman and the Finnish Communications Regulatory Authority are responsible for the supervision of the cross-border data exchange. The Ministry of Transport and Communications supervises the activities of the aforementioned organs.

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 Finnish Communications Regulatory Authority and the Data Protection Ombudsman are in charge of monitoring compliance with the national rules. They exercise their functions under the supervision of the Ministry of Transport and Communications. The Parliamentary Ombudsman supervises the compliance in general, however, the aim is not to increase the working amount of the Parliamentary Ombudsman.

The supervision mainly consists of control of legality. The Finnish Communications Regulatory Authority may issue further orders on the technical implementation of the retention obligations.

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?**

Yes.

If so, please answer to the following questions:

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

The Supreme Administrative Court of Finland, case KHO 18.1.2007/121.

Plaintiff: Private Person A

Defendant: Ministry of the Interior (112info-system)

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

Relevant legal norms in the case were Sections 10 and 12 of the Finnish Constitution, as well as Sections 5, 7 and 16 of the Act on the Openness of Government Activities.

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

The Supreme Administrative Court stated that the secrecy of correspondence, telephony and other confidential communications is secured in the Finnish Act on the Openness of Government Activities. The relevant documents were, according to the court, governmental documents as defined in the Act on the Openness of Government Activities.

The 112info-system could not be considered as a network service in accordance with the Act on the Protection of Privacy in Electronic Communications. Therefore, the confidentiality clause of the Act was not applicable to the case. However, providing the information was at the authorities' discretion, and therefore the court rejected the plaintiff's appeal.

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

No.

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?

According to the Communications Market Act, a public authority shall implement at its own expense a system with which it may receive and handle the information. The public authority shall also be responsible for the costs of connecting the system to a communications network.

The Personal Data Act states that the controller shall carry out the technical and organisational measures necessary for securing personal data against unauthorised access, against accidental or unlawful destruction, manipulation, disclosure and transfer and against other unlawful processing. The techniques available, the associated costs, the quality, quantity and age of the data, as well as the significance of the processing to the protection of privacy shall be taken into account when carrying out the measures.

The obligation to retain data is directed at the service provider. However, the service provider shall organize the storage of data either itself or in cooperation with a network operator.

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?

According to the customer service of the Data Protection Ombudsman, Finnish authorities cannot oblige other authorities in foreign countries (EU or the others) to store data for their purposes, nor can they have influence on what data should be stored. The implementation of the Directive and the content of the data retention regulation are under the decision-making procedure of the foreign country in question. As these procedures vary, it is difficult to provide the question with an exhaustive answer, and instead only to mention that in data retention, the authorities have to apply the national data security rules.

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

a) no data are retained beyond what is permitted?

The sections concerning a corporate or association subscriber's right to process data in cases of misuse (Act on the Protection of Privacy in Electronic Communications, Section 13 a), a telecommunications operator's and value added service provider's right to process data in cases of misuse (Section 13) and a corporate or association subscriber's right to process data in cases of misuse specify these issues.

Coercive measures (Section 41), penal provisions (Section 42) as well as the possibility to appeal (Section 43) are applicable as well.

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)?

The Finnish Communications Regulatory Authority and the Data Protection Ombudsman (Section 41) are responsible for the supervision.

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

Please see answer to question 40 a.

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.

Coercive measures (Section 41), penal provisions (Section 42) as well as the possibility to appeal (Section 43) are applicable.

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

Coercive measures (Section 41), penal provisions (Section 42) as well as the possibility to appeal (Section 43) are applicable.

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

Please see answer to question 18 (Sections 24 and 25 of the Personal Data Act).

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

According to the Personal Data Act, the Data Protection Ombudsman provides direction and guidance on the processing of personal data, supervises the processing in order to achieve the objectives of this Act, as well as makes decisions, as provided in this Act. The Data Protection Board deals with questions of principle relating to the processing of personal data, where these are

significant to the application of the act, as well as makes decisions in matters of data protection.

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 Finnish Communications Regulatory Authority shall supervise compliance with the Act.

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?

For example, the prohibitions on defamation and invasion of privacy, protection of privacy. Guidelines can be found on the Internet pages of the Finnish Communications Regulatory Authority. (See: http://www.tietoturvaopas.fi/en/index/perusohjeet.html).

Standards relating to risk analysis, commitment of the board, classification of data, file descriptions and definition of authorities to use can be found on the Internet pages of the Ministry of Finance (the relevant documents are available only in Finnish[19]).

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.

Data transmission is performed through digital transmission, through a transmission based on either a connection or a package. The technical implementation must reach the level of "sufficient protection". However, the definition of such level has deliberately been left unspecified, as the level is depending on the situation that

[19] As an overview, the data security instruction concerning the *principles and good practices of the administration of authority to use* (vm 37/01/2006) provided by the Ministry of Finance (more specifically the Government Information Security Management Board VAHTI), has an objective to improve the administration of authority to use and to create a solid base for implementing these principles and practices. The instruction is intended to the management of organisations, persons responsible for data security, persons responsible for personnel and information management as well as to the data system owners and the persons responsible for the function of such data systems. The essential requirement in the good practice is the extensive and continuous work on data security. This instruction is especially referring to organisations using large data systems (instruction in Finnish http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061122Kaeyttoe/vahti_9_06.pdf, other relevant document may be found from the website in English http://www.vm.fi/vm/en/01_main/index.jsp).

varies due to constant developments and to differences in the form and content of protection[20].

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?

According to the same procedure as defined above in the description of the national procedure.

There are no references to a common working language, but according to the customer service of the Data Protection Ombudsman and as a general assumption, the most commonly used language is English.

B. National (societal) context

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

The public debate has mainly consisted of articles regarding the subject. (Including articles concerning legal regulation of electronic banking; protection of business secrets and the personnel; obligations of data controller and responsibility of principal; legal policy and research of information society; legislation applicable to service communities; freedom of speech and protection of privacy [Only book available in English was Ms. Riitta Ollila's "Freedom of speech and protection of privacy in convergence of electronic communications" (University of Lapland, 2001)]; legal position of a decedent's e-mail; and regulation of direct marketing.)

---

[20] There may be found information security guidelines and other policy guidelines concerning the general aspects of technical and/or organisational measures provided by the Ministry of Finance and Government Information Security Management Board, as especially the Board functions within the area of information security concerning administrative security, personnel security, physical security, security of telecommunications services, hardware and equipment security, software security, security of information material, operations security, risk management and contingency planning. In addition, The Ministry of Finance takes an active part in international co-operation in the field of information security in, for example, the EU, the OECD and ENISA. However, due to the abovementioned rapidity of developments, it is difficult to provide the question with a precise answer.

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)?

Yes, employment data is subject to retention obligation as long as this is necessary for the employer to comply its obligations under the applicable legislation.

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.

Please see the following link:

http://www.cert.fi/en/reports/statistics/autoreporter.html

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?

For example, according to a statement of the Finnish National Institute for Health and Welfare, the retention of data is more accurately regulated.

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

The Finnish Communications Regulatory Authority provides a large amount of different services, surveys and statistics as well as regulations, decisions and guidelines including a wide range of information that additionally indicates the current discussion and development on, for example, data retention. The information can be found from their Internet pages at the following address: http://www.ficora.fi/en/index.html (please see also the most frequently asked questions, which in a way provides the current topics of discussion now days, at the following address: http://www.ficora.fi/en/index/palvelut/ukk.html and the national recommendations and GFI documents relating to telecommunication that can be found at the following address: http://www.ficora.fi/en/index/saadokset/ohjeet/teletoiminta.html).

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the se crecy 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[21] – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a *specific* reason?

The Finnish Constitution protects the following fundamental rights relating to privacy: the right to privacy, the freedom of expression and right of access to information, freedom of religion and conscience, the right to life, personal liberty and integrity, protection of property and protection of basic rights and liberties. The Finnish Constitution regulates these rights as follows:

Section 10 - The right to privacy

Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act. The secrecy of correspondence, telephony and other confidential communications is inviolable. Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act.

Section 11 - Freedom of religion and conscience

Everyone has the freedom of religion and conscience. Freedom of religion and conscience entails the right to profess and practice a religion, the right to express one's convictions and the right to be a member of or decline to be a member of a religious community. No one is under the obligation, against his or her conscience, to participate in the practice of a religion.

Section 12 - Freedom of expression and right of access to information

Everyone has the freedom of expression. Freedom of expression entails the right to express, disseminate and receive information, opinions and other communications without prior prevention by anyone. More detailed provisions on the exercise of the freedom of expression are laid down by an Act. Provisions on restrictions relating to pictorial programmes that are necessary for the protection of children may be laid down by an Act. Documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically

[21] 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).

restricted by an Act. Everyone has the right of access to public documents and recordings.

Section 7 - The right to life, personal liberty and integrity

Everyone has the right to life, personal liberty, integrity and security. No one shall be sentenced to death, tortured or otherwise treated in a manner violating human dignity. The personal integrity of the individual shall not be violated, nor shall anyone be deprived of liberty arbitrarily or without a reason prescribed by an Act. A penalty involving deprivation of liberty may be imposed only by a court of law. The lawfulness of other cases of deprivation of liberty may be submitted for review by a court of law. The rights of individuals deprived of their liberty shall be guaranteed by an Act.

Section 15 - Protection of property

The property of everyone is protected. Provisions on the expropriation of property, for public needs and against full compensation, are laid down by an Act.'

Section 22 - Protection of basic rights and liberties

The public authorities shall guarantee the observance of basic rights and liberties and human rights.

Correspondence, telephony and e-mails, inter alia, are considered as telecommunications content. Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act.

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

The limitations shall be based on a law of the parliament, which shall be accurate and clearly defined, acceptable, shall not affect the very core of the fundamental right, the limitation shall be necessary for achieving the desired goal and in a right proportion to the object of legal protection, there have to be adequate arrangements of legal safeguards, and the international human rights obligations have to be followed.

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

The following rulings of the Finnish Supreme Administrative Court relate to the right to privacy (Section 10 of the Constitution):

KHO 2010:42: The police had requested information concerning medicinal product purchases of individual persons from the Social Insurance Institution of Finland, in order to use it in a criminal investigation concerning a suspected murder. The police was entitled to receive the requested information in accoredance with the Finnish Police Act Sec. 35(1).

KHO 2005:2: In 1999, a foreigner born in the 1982 was permitted a temporary residence permit on the grounds of family relations as an under-aged child of a father living in Finland. When arriving to Finland in 2002, the foreigner had announced his entering into matrimony in his previous country of domicile earlier in 2002. This entering into matrimony was not considered as a weighty reason to cancel the temporary residence permit in accordance with Finnish Aliens Act (378/1991).

KHO 2002:75: When estimating the amount of beds to demented persons, the functional unit providing private social services had to take into account the general living condition requirement and the fundamental rights of the residents, e.g. protection of privacy. It was not considered reasonable to accommodate two non-related and unfamiliar persons in a single room. Neither was this justified by financial matters.

These rulings have deviated from each other with regard to the weight of the *right to privacy*, and the Finnish Supreme Administrative Court has ruled both in favour of and against this constitutional right. Notwithstanding the lack of explicit rulings concerning directly the Act in question, the transposition of the Directive has been carried out successfully.

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 and therefore a balance of interest is carried out in each individual case. Please see also answer to the question 51.

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)?

According to the Personal Data Act, the processing of sensitive data is prohibited. Personal data are deemed to be sensitive, if they relate to or are intended to relate to race or ethnic origin, the social, political or religious affiliation or trade-union membership of a person, a criminal act, punishment or other criminal sanction, the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person, the sexual preferences or sex life of a person, or the social welfare needs of a person or the benefits, support or other social welfare

assistance received by the person. However, there are several exceptions to this main rule.

II. Dimension 2 (State – economy)

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

The freedom of expression and right of access to information are potentially restricted. In case it would be considered that the fundamental rights of the obligated parties have been violated, Section 21 concerning protection under the law can be applied.

According to the Government Bill (HE 158/2007), the restrictions are, however, in line with constitutional law. The limits to the restrictions fall within the scope of the general restriction conditions of the fundamental rights described above in the answer to question 51.

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)?

According to the Finnish Constitution, a public administrative task may be delegated to others than public authorities only by an Act or by virtue of an Act, if this is necessary for the appropriate performance of the task and if basic rights and liberties, legal remedies and other requirements of good governance are not endangered. However, a task involving significant exercise of public powers can only be delegated to public authorities.

For the purposes of authorities, for the purposes of investigating disclosures of business secrets, for investigating unauthorized use of information society service, communications network or communications service, or the right to process data in case of misuse law allows to draw up on private actors for the purposes of data retention. The general restriction conditions of the fundamental rights (please see answer to question 51) shall also be applied.

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

According to constitutional law, only expropriation of property shall be carried out against full compensation. However, according to the preparatory works of the Act on the Protection of Privacy in Electronic Communications, i.e. the law transposing

the Directive, the costs relating to the fulfilment of the retention obligation is reimbursed by the authority whose purposes the data is stored for.

III. Dimension 3 (State – State)

58. What status do international treaties and, in particular, the European Convention on Human Rights (ECHR) have within the hierarchy of norms of your country's legal system?

International agreements and other international obligations, to which Finland is committed, are binding sources of law in Finland. The practice of the international bodies which apply such agreements also has significance as a source of law. One example of a source of law which belongs to this category is the Convention of the Council of Europe on Human Rights, and the practice of the European Court of Human Rights is relevant to the interpretation of the Convention.

International agreements have the same hierarchical ranking as the instrument used to implement them in Finland. Thus, if an international agreement is implemented by an act, the provisions of that agreement have the hierarchical ranking in Finland of the provisions of an act.

The Finnish Constitution shall be in harmony with the European Convention on Human Rights, among others. International treaties are legally binding in Finland only when enforced through a parliamentary law (dualistic system). The international treaties are higher than the constitution in the hierarchy of norms, although national legislation is harmonized with the treaties when they are brought into force nationally.

Should a conflict rise between the Constitution and other provisions, an attempt is made to resolve it by means of interpretation. Thus, efforts are made to interpret legislation and other provisions in order to remove the conflict with the Constitution. Where international human rights obligations are concerned, the Constitutional Law Committee has espoused the principle according to which, where alternative interpretations can be justified, the alternative to be adopted should be the one which furthers the realisation of provisions on human rights, in other words the alternative that is deemed to be human-rights-friendly. The underlying principle is, therefore, that legislation drawn up in Parliament must comply with the Constitution and international agreements on human rights.

In accordance with doctrine on the supremacy of European Union law, Union law takes precedence over national law. Therefore, where a national provision and a binding provision of Union law are incompatible with each other, the provision of Union law will have precedence, also in the case of Finnish Constitution.

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?

As a Member of the European Union, Finland is of course also bound by Union law. Regulations and directives are among the most important legislation of the European Communities. Directives must be implemented in Member States. Preliminary work for the implementing legislation may therefore also have interpretative significance with regard to how Community law is interpreted.

Finland has implemented a dualist system, in which international Agreements do not directly become binding domestically until they have been specifically implemented domestically. The Constitution states that international obligations falling within the scope of legislation are to be implemented by an act of Parliament. Other provisions are to be implemented by decree. An international obligation enters into force domestically at the time provided for in the implementing provisions. International agreements, which are binding on Finland and the provisions implementing them, are published in the Treaty Series of the Statute Book of Finland.

In order for legislation to be enacted in the form of an act, it must be presented to Parliament for consideration as a Government proposal or as an initiative by a Member of Parliament. Government proposals are prepared within the Ministries and are subsequently discussed by them at the Government plenary session. After that, a decision on bringing the Government proposal before Parliament is made at the Presidential session.

In Parliament a Government proposal is first the subject of a preliminary debate, after which it is assigned to a Parliamentary Committee for consideration. The Committee hears experts and drafts a report on the Government proposal. The matter is then referred to the plenary session of Parliament where the report of the Parliamentary Committee acts as a basis for discussion of the matter. The decision to pass bills is taken at a plenary session of Parliament in two readings. Parliament may pass a bill without amending it, amend it or reject it. The final power of decision on the fate of a bill therefore lies with Parliament. Ordinary bills are passed in Parliament by means of a simple majority, whereas an amendment to the Constitution requires a stipulated majority. Once a bill has been passed by Parliament, it is forwarded to the President of the Republic for approval. An act enters into force at the time specified in its provision on entry into force, but in any event does not enter into force before it has been published in the Statute Book of Finland.

Decrees issued by the President of the Republic, the Government or a Ministry are prepared in the Ministry which deals with the matter concerned. Where presidential decrees are concerned, the President of the Republic makes a decision to issue a decree acting on proposals presented by the Government. The issuing of government decrees is determined at government plenary sessions, and the issuing of ministerial decrees is determined by the ministry concerned. All decrees are published in the Statute Book of Finland. A decree enters into force at the time specified in the decree itself, but in any event does not enter into force before the decree has been published in the Statute Book.

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?

In accordance with doctrine on the supremacy of European Union law, Union law takes precedence over national law. Therefore, where a national provision and a binding provision of Union law are incompatible with each other, the provision of Union law shall have precedence, also over the Finnish Constitution. Thus, the EU can exercise competence already transferred even when this competence would be in conflict with national law. However, as mentioned above, Finland is one of the dualist system countries in which international agreements do not directly become binding domestically until they have been specifically implemented domestically.

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?

General guidance and development for the purpose of implementing the Act on the Protection of Privacy in Electronic Communications is the responsibility of the Ministry of Transport and Communications. The Finnish Communications Regulatory Authority and the Data Protection Ombudsman answer for the supervision of compliance with the provisions of the Act.

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

According to the Personal Data Act, personal data may be transferred to outside the European Union or the European Economic Area only if the country in question guarantees an adequate level of data protection. Personal data may be transferred out of the territory of the member states of the European Union or out of the European Economic Area, if the Commission of the European Communities has found that the country in question guarantees an adequate level of data protection.

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?

The exceptions to the processing of sensitive data are quite exhaustive. Although the main rule according to the Finnish Personal Data Act is that processing of sensitive data is prohibited, there are numerous situations where information on the object of sensitive data is revealed on the basis of a special provision. This is an issue which could be addressed in more detail, and perhaps also more actively

debated, because in the current situation the legal safeguards of the data object are very limited with regard to sensitive data.

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

Finland

Anne Yliniva-Hoffmann

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*?

Yes, Sec. 12 of the Constitution of Finland[1], which rules the following[2]:

> *Section 12 - Freedom of expression and right of access to information*
> *Everyone has the freedom of expression. Freedom of expression entails the right to express, disseminate and receive information, opinions and other communications without prior prevention by anyone. More detailed provisions on the exercise of the freedom of expression are laid down by an Act. Provisions on restrictions relating to pictorial programmes that are necessary for the protection of children may be laid down by an Act. Documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings.*

is seen to include the right to anonymous expression of opinion/messages, too[3].

---

1 The Constitution of Finland 731/1999 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf

2 A/N: all information given in this questionnaire base on the Finnish versions of the relevant regulations; it is made reference to the English-language documents, as far as these are available, but it should be noted that these are unofficial translations which oftenly do not include the most current amendments in force.

3 See the research of *Päivi Tiilikka* on commission of the Ministry of Justice available in Finnish at: http://www.om.fi/Satellite?blobtable=MungoBlobs&blobcol=urldata&SSURIapptype=BlobServer&SSURIcontainer=Default&SSURIsession=false&blobkey=id&blobheadervalue1=inline;%20filename=OMML%2054%202010%20selvitys.pdf&SSURIsscontext=Satellite%20Server&blobwhere=1277811184388&blobheadername1=Content-Disposition&ssbinary=true&blobheader=application/pdf

In addition to this, Sec. 16 of the Act on the Exercise of Freedom of Expression in Mass Media 460/2003[4] determines the confidentiality of sources and the right to anonymous expression as far as messages, provided to the public are concerned. According to Sec. 3 of Act 460/2003 Sec. 16 applies – besides of publishing and broadcasting – also to a private individual, who maintains a web site on an electronic communications network. These provisions shall underline the essential importance of the confidentiality of sources as well as the right to anonymous expression – as independently of each other to be protected rights – for the functionning of the media and the performance of the media´s public tasks[5]. According to Sec. 17 of Act 460/2003 a court may – upon request and under circumstances specified in this provision – order the the keeper of a transmitter, server or other similar device to release information required for the identification of the sender of a certain network message. Unlike Sec. 16, Sec. 17 does not apply to a private individual´s website as mentioned above, but only to the other persons/entities mentioned in Sec. 3.

In this context a decision of the ECHR (*Case of K.U. vs. Finland*[6]) should be mentioned. In this case the minor applicant had – unknown to him – been the subject of an advertisement of a sexual nature on an Internet dating site. Subsequntly to this advertisement he was contacted by a man who expressed his sexual interests to him. The identity of the person who had placed the advertisement could not be obtained from the Internet provider due to the legislation in place at that time. The concerned Finnish courts found that there was no explicit legal provision authorising them to order the service provider to disclose telecommunications identification data in breach of professional secrecy. The ECHR found that there had been a violation of Art. 8 ECHR due to the lack of relevant legislation guaranteeing an effective protection of the applicant´s rights.

---

4 The Act on the Exercise of Freedom of Expression in Mass Media 460/2003 provides more detailed provisions on the freedom of expression as guaranteed in the Constitution (Sec. 1); it is available in English at: http://www.finlex.fi/fi/laki/kaannokset/2003/en20030460.pdf

5 See Government proposal to the Parliament on the Exercise of Freedom of Expression in Mass Media HE 54/2002 vp available in Finnish at: http://edilex.fi/virallistieto/he/fi20020054.pdf

6 The Decision of the ECHR of 2 December 2008 (Application no. 2872/02) refers, however, to the legal situation before the Act 516/2004 was issued; it is available at: http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=Finland&sessionid=79824739&skin=hudoc-en

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 July 2011 Act 855/2011[7] Amending the Act on the Protection on Privacy in Electronic Communications (516/2004[8]) was adopted. It will enter into force on 1 January 2014.

The Act 855/2011 is based on Government Bill HE 222/2010[9] of 29 October 2010, titled "Government Bill proposed to the Parliament on a Reform of the Criminal Investigations and Coercive Measures Legislation." The Bill proposed to replace the existing Criminal Investigations Act[10] and Coercive Measures Act[11]. Furthermore it entailed amendments to other legislation connected to the two Acts to be replaced and explicitly took reference to the then proposed reform of the Police Act.

According to the explanatory notes of the Bill the aim of the reform is to govern the powers of the responsible authorities more accurately and comprehensively while taking into account the protection of fundamental and human rights as well as the needs of crime prevention. It is emphasised that the partial amendments that have been made in the past have kept legistlation up-to-date, but particularly with regard to the so called secret investigation measures (i.e. measures taken unknown to the subject) provided for in the Coercive Measures Act and the provisions concerning

---

7 The Act Amending the Act on the Protection on Privacy in Electronic Communications 855/2011 is available in Finnish at: http://www.finlex.fi/fi/laki/alkup/2011/20110855

8 The Act on the Protection on Privacy in Electronic Communications 516/2004 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf

9 The Government Bill HE 222/2010 is available in Finnish at: http://www.finlex.fi/fi/esitykset/he/2010/20100222

10 The existing Criminal Investigations Act 449/1987 is available in Finnish at: http://www.finlex.fi/fi/laki/alkup/1987/19870449?search[type]=pika&search[pika]=esitutkintalaki; it will be replaced by the Criminal Investigations Act 855/2011 which was adopted on 22 July 2011 and will enter into force on 1 January 2014 and is available in Finnish at: http://www.finlex.fi/fi/laki/alkup/2011/20110805

11 The existing Coercive Measures Act 450/1987 is available in Finnish at: http://www.finlex.fi/fi/laki/alkup/1987/19870450; the Coercive Measures Act 806/2011 was adopted on 22 July 2011 and will come into force on 1 January 2014, it is available in Finnish at: http://www.finlex.fi/fi/laki/alkup/2011/20110806; an English version of the Act 450/1987 (as of 1997) can be received from the Finnish Ministry of Justice and is attached to this document.

the gathering of information as to Chapter 3 of the Police Act 493/1995[12] a partly confusing and rather awkward to handle set of regulations has arisen. Particularly with regard to the secret investigation measures (eavesdropping, telecommunications monitoring and technical surveillance) the relevant provisions shall be able to answer to the challenges resulting from technical development.

In this context it is stressed that according to Sec. 2 para 3 of the Constitution of Finland[13] the exercise of public powers shall be based on an Act and in all public activity the law shall be strictly observed (rule of law). The consideration of fundamental and human rights becomes even more important when it is about secret investigations which oftenly trench upon the core content of constitutional rights. These constitutional rights, however, have to be balanced against the requirements of an efficient crime prevention. The prevention of crime and other harmful events has to be seen as a part of the protection of fundamental and human rights, too. Nevertheless the rule of law requires that all provisions allowing for secret investigation measures have to determine the respective premises very precisely. Besides this – and with reference to the jurisdiction of the ECHR – the principle of subsidiarity and the requirement of an independent subsequent control mechanism have to be observed.

With regard to data retention aspects the following is explained. The new Coercive Measures Act provides for new investigatory actions, as device-targeted search techniques, i.e. measures that aim at the acquisition of information content on computers, telecommunications terminals or other similar technical devices. Furthermore the Coercive Measures Act will include several secret investigation measures, some of which are new, too. These secret measures are for example telecommunications interception, telcommunications monitoring, systematic surveillance, undercover gathering of information, technical surveillance, obtaining of identification data concerning the address or terminal device of telecommunications, undercover activities and transactions, the use of human intelligence resources and controlled delivery. The obligation to report on secret coercive measures and the conditions when to refrain from it shall be governed in more detail.

According to Act 855/2011 the following Sections of Law 516/2004 will be changed:

- Sec. 36 (*Certain other authorities right of access to information*) para 3 will be repealed:

  (3) Notwithstanding the obligation of secrecy provided in section 5, the police are entitled to receive from a telecommunications operator:

---

[12] The existing Police Act 493/1995 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1995/en19950493.pdf

[13] The Constitution of Finland 731/1999 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf

1) identification data on transmissions to a particular subscriber connection, with the consent of the injured party and the possessor of the subscriber connection, necessary for the purpose of investigating a violation of a restraining order referred to in Chapter 16(9a) of the Penal Code, criminal disturbance referred to in Chapter 17(13)(2) of the Penal Code or breach of domestic peace referred to in Chapter 24(1)(3) of the Penal Code; and (686/2009)
2) identification data on messages transmitted from a particular mobile communications device, with the consent of the subscriber or owner of the device, insofar as necessary for investigating a crime where the mobile communications device or the subscriber connection used therein has been unlawfully in the possession of another party.

This paragraph is seen to become redundant when the provisions on telecommunications monitoring in the new Coercive Measures Act/Police Act enter into force.
The amendment results from the overlapping in the existing Acts as mentioned above; e.g. according to Chapter 5a Sec. 1 (2) of the present Coercive Measures Act telecommunications monitoring means:

the obtaining of secret identification data on telemessages that have been sent from a subscription, telecommunications address or a telecommunications terminal equipment connected to a communications network referred to in paragraph 1 [AN: which refers to the Communications Market Act (393/2003)], or received at such a subscription, telecommunications address or telecommunications terminal equipment, and the obtaining of location data of mobile stations and the temporary disconnection of such a subscription or telecommunications terminal equipment;

While according to Chapter 3 Sec. 28 (1) 6 of the present Police Act telecommunications monitoring means:

the obtaining of secret identification data on telemessages that have been sent from a subscription, e-mail address or another telecommunications address or a telecommunications terminal equipment connected to a public communications network or a communications network linked with the public communications network referred to in the Communications Market Act (393/2003), or received at such a subscription, telecommunications address or telecommunications terminal equipment, and the obtaining of location data of mobile stations and the temporary disconnection of such a subscription or telecommunications terminal equipment;

The differences between both rules are assumed to be unreasonable, therefore telecommunications monitoring shall be determined coherent. This happens in Chapter 10 Sec. 6 (1) of the new Coercive Measures Act 806/2011 and Chapter 5 Sec. 8 (1) of the new Police Act 872/2011, both of which reference to the definition of “identification data” in Sec. 2 (8) of the Act on the Protection of Privacy in Electronic Communications (516/2004). Chapter 9 Sec. 36 (1) of Act

516/2004 refers explicitly to the Coercive Measures Act and the Police Act. The confidentiality of messages will still be regulated generally in Sec. 4 (1) and (2) of Act 516/2004.

- Sec. 14a (*Obligation to restore data for the purposes of the authorities*) para 1 rules:

  (1) Notwithstanding the provisions of this Chapter concerning the processing of identification data, a service operator obliged to submit a telecommunications notification shall ensure, under the conditions prescribed below, that data referred to in Article 5 of the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC are retained for a period of 12 months from the date of the communication. Such data may be used only for the purposes of investigating, solving and considering charges for criminal acts referred to in Chapter 5 a(3)(1) of the Coercive Measures Act (450/1987).

  In its new version it will refer to Chapter 10 Sec. 6 para 2 Coersive Measures Act (806/2011[14]). Chapter 5a Sec. 3 para 1 of the existing Coercive Measures Act lists the following criminal acts a person has to be suspected of:

  1.) a criminal offence for which the maximum penalty is at least four years' imprisonment;

  2.) an offence against an automatic data processing system using a telecommunications terminal device, procurement, threat against a person who shall be heard in a legal procceding, illegal threat or drug offense;

  3.) an indictable attempt of an offence referred to above;

  4.) the preparation of a crime with a terroristical intention;

  5.) a grievious offence against provisions on customs clearance or

  6.) a grievious concealing pouched game (i.e. a natural resources offence).

  Chapter 10 Sec. 6 para 2 of the new Coercive Measures Act 806/2011 shows some differences. The criminal acts listed there are the following:

  1.) the same as before;

  2) an offence commited by using a telecommunications address or a telecommunications terminal device, if the maximum penalty for the offence is at least two years´ imprisonment;

  3.) the sexual exploitation of a person or procurement;

  4.) a drug offence; 5.)-7.) correspond to 4.)-6.) of the existing version.

---

[14] The new Coercive Measures Act 806/2011 was adopted on 22 July 2011 and will come into force on 1 January 2014; it is available in Finnish at: http://www.finlex.fi/fi/laki/alkup/2011/20110806

- Sec. 14b (*Obligations and procedures for processing data retained for the purposes of the authorities*) para 2 rules:

  (2) Provisions on compensation for costs incurred by fulfilling the retention obligation and preparing for it are laid down in section 98 of the Communications Market Act. Provisions on retaining data for the purpose of investigating a single crime are laid down in Chapter 4(4 b and c) of the Coercive Measures Act.

  In its new version it will refer to Chapter 8 Sec. 24-26 Coercive Measures Act. The new provisions include some supplements to the existing ones, regarding the official order to retain data: it is added that the officials educated assumption, that the data which shall be retained are relevant for the respective investigation shall be on hand before the conduction of a device-search (Chap. 8 § 24 Sent. 1) and that the written order shall specify the data concerned (Chap. 8 § 24 Sent. 3). Furthermore it is foreseen that the order as well as its renewal shall be imposed for a period of three months at a time (Chap. 8 § 25 Sent. 1) and shall be repealed as soon as it is not needed anymore (Chap. 8 § 25 Sent. 2).

- Sec. 14c (*Statistics concerning the use of data to be retained for the purposes of the authorities*) para 2 rules:

  (2) The Ministry of the Interior shall in particular take the statistics referred to above in subsection 1 into account in its reports about telecommunications interception and monitoring to Parliamentary Ombudsman by virtue of the Police Act (493/1995), Coercive Measures Act or any other Act.

  In its new version it will take reference to the new Police Act 872/2011[15]. This change is necessary due to the amendments to the latter one.

- The same applies to Sec. 95 (*Obligation of a telecommunications operator to equip its systems for telecommunications interception and monitoring)* of the Communications Market Act 393/2003[16]. This provision is amended by Act 857/2011[17], adopted on 22 July 2011 and coming into force on 1 January 2014, and will then refer to the new Coercive Measures Act and the new Police Act.

Further legislative amendments are – according to the publicly available official information – not under way at the present.

With regard to public discussion on data protection topics, these mostly concern data protection in working life, particularly the so called Lex Nokia which in 2009

---

[15] The new Police Act 872/2011 was adopted on 22 July 2011 and will come into force on 1 January 2014; it is available in Finnish at: http://www.finlex.fi/fi/laki/alkup/2011/20110872

[16] The Communications Market Act 393/2003 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/2003/en20030393.pdf

[17] The Act amending Section 95 of the Commuications Market Act 393/2003 is available in Finnish at: http://www.finlex.fi/fi/laki/alkup/2011/20110857

introduced the then new Sec. 12 a, 13 a—13 k into Act 516/2004. It can be noted that the Directive and its transposition into Finnish legislation did not face broader discussion.

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

   The Coercive Measures Act 450/1987 determines the following obligations:

   - Chapter 4 "*Seizure*" of objects, documents or data relevant for criminal proceedings or the investigation of criminal offenses. Sec. 4 obliges the office concerned to stop the transmission of a letter, another postal shipment, telegram or shipment of goods, which is en route to an office of the postal and telecommunications service, a railways operating point, an office for scheduled traffic by motor vehicle, ship or cargo aircraft or an office for the handling of goods transported in such traffic, in order to enable the official seizure of the respective object. This order may be imposed for one month at the longest. According to Sec. 4a an information system manager, administrator or other person is obliged to provide the investigation authority, upon its request, the passwords or other similar information the obliged person is aware of, which are necessary for the seizure.

   - Chapter 5 "*Search*" of premises and persons, inter alia for the investigation of criminal offences the maximum penalty of which is at least six months imprisonment (Sec. 1 and 10). Sec. 1 (2) and 2 (2) allow for a search of premises of a person other than the suspect, under certain circumstances.

   - Chapter 5a determines the investigation authority´s powers with regard to "*Telecommunications interception, telecommunications monitoring and technical surveillance*". The different measures have varying conditions (e.g. regarding the criminal offences the person is suspected of) and include several obligations of telecommunications companies to support these official measures. Sec. 3a entitles the official to access to location data of mobile communication equipment deemed to be relevant for the investigation of a criminal offence as provided for in Sec. 3 (which applies to data retention according to Sec. 14a Act 516/2004, too). Sec. 9 obliges the telecommunications company to support the investigating official technically, personelly and with the needed information and equipment, as far as this is necessary for the conduction of telecommunications interception, telecommunications monitoring and technical surveillance measures.

The Police Act 493/1995[18] determines the following obligations in Chapter 3 "*Provisions on gathering information*". With regard to telecommunications interception, telecommunications monitoring and technical surveillance measures Sec. 28 (2) makes a reference to what is said in the Coercive Measures Act. Sec. 31c-e of the Police Act describe the conditions under which telecommunications interception and monitoring are (not) permitted. Sec. 31f entitles the police to access to location data of mobile communication equipment deemed to be relevant for the investigation of a criminal offence as provided for in Sec. 31 (which most closely corresponds to what is said in Chapter 5a Sec. 3 of the Coercive Measures Act). Sec. 36 (*Obtaining information from a private organisation or person*) says the following:

> *(1) At the request of a commanding police officer, the police have the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members or employees of an organisation. The police have the same right to obtain information needed in a police investigation under section 37 if an important public or private interest so requires.*
> *(2) The police have the right to obtain from a telecommunications operator and a corporate or association subscriber, or by using a technical device, the contact information about a subscription that is not listed in a public directory or the data specifying a telecommunications subscriber connection, an e-mail address or other telecommunications address, or telecommunications terminal equipment if, in individual cases, the information is needed to carry out police duties. Similarly, the police have the right to obtain postal address information from organisations engaged in postal services. In order to obtain the information, the police may only use technical devices that can be used solely for specifying subscriptions and telecommunications terminal equipment. [...]*
> *(3) For licence administration purposes, the police have the right to obtain information from*
> *private organisations and persons as provided in section 35(2-5).*
> *(4) Separate provisions apply to telecommunications interception, telecommunications*
> *monitoring and gathering information on the location of mobile stations.*

The Border Guard Act 578/2005[19] determines in Chapter 6 Sec. 41 the "*Powers of border guardsmen to prevent and investigate offences*" in the border guard´s area of responsibility (Sec. 42). These refer for the most part to the powers the police has according tot the Police Act, the Coercive Measures Act and the Criminal Investigations Act, but makes certain restrictions with regard to undercover activities, undercover transactions, telecommunications interception and monitoring. Sec. 41 (2) says that what is provided for the police´s right of access to location data

---

[18] The Police Act 493/1995 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1995/en19950493.pdf

[19] The Border Guard Act 578/2005 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/2005/en20050578.pdf

of mobile communication equipment (see above) applies to the border guard, too. Sec. 41 (3) rules that the provisions on the powers of commanding police officers to prevent and investigate offences and to bring charges apply to officials with the right to make an arrest and to heads of investigation in the Border Guard. Chapter 3 Sec. 36 of the Police Act (see above) falls within the commanding police officer´s remit.

The Criminal Investigations Act 449/1987[20] provides for general cooperation-obligations as e.g. being available for hearings as witness or defedant (Sec. 17 et seq.). The same is true with regard to Chapter 17 Sec. 18 et seq. of the Code of the Judicial Procedure 4/1734[21] on the duties and rights of witnesses.

The Act on the Processing of Personal Data by the Border Guard 579/2005[22] determines in Sec. 18 the border guards powers on gathering information corresponding to those of the police as provided for in Chapter 3 Sec. 36 of the Police Act (see above) concerning criminal offences in the border guards field of competence.

The Customs Act 1466/1994[23] provides in Sec. 28 for the customs authority´s right to obtain information from certain registers. Sec. 28 (3), (4) award the customs authority the right to obtain any information necessary to prevent or investigate a customs offence, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members or employees of an organisation, as well as the right to obtain from a telecommunications operator the contact information about a subscription that is not listed in a public directory. Similarly, the customs authority has the right to obtain postal address information from organisations engaged in postal services.

The Act on Foreign Trade and Monitoring and Protection Measures in Certain Cases 1521/1994[24], which inter alia refers to customs aspects, determines in Sec. 8 (2) the obligation of importers, exporters and other persons having relevant information on imports/exports to provide the responsible official upon request their relevant documents, correspondence or other information necessary for the monitoring.

---

20 The Criminal Investigations Act 449/1987 is available in Finnish at: http://www.finlex.fi/fi/laki/ajantasa/1987/19870449

21 The Code of the Judicial Procedure 4/1734 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1734/en17340004.pdf

22 The Act on the Processing of Personal Data by the Border Guard 579/2005 is available in Finnish at:

23 The Customs Act 1466/1994 is available in Finnish at: http://www.finlex.fi/fi/laki/ajantasa/1994/19941466

24 The Act on Foreign Trade and Monitoring and Protection Measures in Certain Cases 1521/1994 is available in Finnish at: http://www.finlex.fi/fi/laki/ajantasa/1994/19941521

In order to prevent money collection offences (Sec. 25) the Money Collection Act 255/2006[25] determines in Sec. 28 the responsible officials rights to obtain information relating to the arrangement of money collections and information needed for the supervision of the arrangement of money collections, inter alia notwithstanding the secrecy obligation laid down in Sec. 94 of the Act on Credit Institutions 1607/1993, from a deposit bank in which the money collection bank account or some other bank account of the permit holder is held.

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 Code of Judicial Procedure 4/1734[26] includes in its Chapter 17 the provisions on evidence, particularly in Sec. 18 et seq. the provisions on witnesses, in court proceedings. Sec. 18 determines which persons may / may not (as party, injured or accused or sentenced) be heard as witness.

Sec. 20 determines the witnesses obligation to testify and names the persons which shall not against their will be questioned (due to marriage, engagement, near relationship, relationship by marriage).

Sec. 23 determines which persons must not testify as witnesses due to their professional positions, as e.g. an attorney or counsel, in respect of what the client has entrusted to him or her for the pursuit of the case.

Sec. 24 provides for the right to refuse to testify in certain cases, as such in which the witness would incriminate him-/herself or a person of a relationship as mentioned in Sec. 20 or the identity of a source of information shall be protected.

The prohibition to testify according to Sec. 23 refers to the relevant information the named persons receive when exercising the professional tasks with regard to the particular mutual trust. According to the jurisdiction of the Finnish Supreme Court (on Sec. 23 (4)) the provision shall be read closely to its wording since it establishes an exception to the general obligation to testify[27]. In favour of these persons also the Coercive Measures Act 450/1987 and the Police Act 493/1995 prohibit certain

---

[25] The Money Collection Act 255/2006 is avaliable in English at: http://www.finlex.fi/fi/laki/kaannokset/2006/en20060255.pdf

[26] The Code of Judicial Procedure 4/1734 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1734/en17340004.pdf

[27] See decision of the Supreme Court KKO:2003:119 as of 3. December 2003, available at: http://www.finlex.fi/fi/oikeus/kko/kko/2003/20030119

investigation measures: according to Chapter 4 Sec. 2 of Act 450/1987 the seizure of documents (the same applies to data) containing information, which fall within the scope of Sec. 23 or 24 of Code 4/1734; according to Sec. 4a Act 450/1987 the information system holder´s obligation to provide the investigation authority the necessary passwords or similar information[28]; according to Chapter 5a Sec. 10 Act 450/1987 concerning telecommunications and technical interception measures (Sec. 31e of Act 493/1987 makes a partly reference to this provision).

In this context it has been criticised[29] that the Code of Judicial Procedure would not recognize the confidential contents of the message or other communication-related information as such, on which it may not be testified in court proceedings. In Government Bill HE 222/2010[30] it is declared that Chapter 17 of the Code of Judicial Procedure 4/1734 is in need of reform, due to the application of secret investigation measures and the utilisation of the findings resulting from these.

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?

- Firstly, Chapter 5 of Act 516/2004 includes provisions on the information security in communications. Sec. 19 rules that telecommunications operators, value added service providers and corporate or association subscribers are responsible for maintaining information security in their services or processing, which explicitly applies to the processing of data for the purposes of the retention obligation (Sec. 14a), too. Sec. 20 determines the measures the obligated parties may take in this context and Sec. 21-21b describe the respective information obligations as well as the tasks of FiCoRA. Based on the Sec. 19 and 20 of Act 516/2004 FiCoRA has issued a regulation on information security management addressed to telecommunications companies[31].

- Following to that, Chapter 9 of Act 516/2004 treats the right of access to information. Sec. 33 provides for the guidance and supervision authorities right to access information. It determines the kind, scope and purpose of the respective information, to which the Ministry of Transport and Communications, the FiCoRA and the Data Protection Ombudsman have the right of access. Beyond that Sec. 33 includes an obligation to destroy certain information and data, when these are no longer needed. Subsequent to this Sec. 34 regulates the supervision authorities´ obligation of secrecy and makes a reference to the

---

28 See in this context Government Bill HE 153/2006 vp (p. 70), available in Finnish at: http://www.eduskunta.fi/triphome/bin/thw/?${APPL}=akirjat&${BASE}=akirjat&${THWIDS}=0.25/1318800145_125166&${TRIPPIFE}=PDF.pdf

29 See: http://www.ficom.fi/lausunnot/index_1.html?Id=1299601971.html&Tulosta=1

30 See Government Bill HE 222/2010, p. 114; available in Finnish at: http://www.edilex.fi/virallistieto/he/fi20100222.pdf

31 The Regulation 47 C/2009 M of 27 August 2009 is available in English at: http://www.ficora.fi/attachments/englantiav/5k8y6zm5w/FICORA47C2009M.pdf

general secrecy obligations according to Chapter 6 of the Act on the Openness of Government Activities 621/1999[32]. The following Sec. 34a allows for the disclosure of information held by the mentioned authorities in certain cases.

- On 12 May 2011 a Government Decree[33] has been issued by virtue of Sec. 14b (3) of Act 516/2004. The Decree shall specify how the retention obligation of Sec. 14a Act 516/2004 can be met. According to Sec. 1 of Decree 503/2011 the Ministry of Interior may acquire from a third service provider a system, to which the according to Sec. 14a of Act 516/2004 obliged provider may transfer the stored data[34]. The obliged provider is then to be seen as the responsible controller of the register pursuant to Sec. 3 (1) no. 4 of the Personal Data Act 523/1999[35]. According to Sec. 2 of the Decree the obliged provider is allowed to store in this register also data the provider still needs for its own purposes. The Decree entered into force on 1 June 2011 (Sec. 3).

- Sec. 36 of Act 516/2004 on certain other authorities right of access rules that data to be retained under Sec. 14a is only obtainable from service providers by those authorities which have a legal right to obtain these. This provision does neither say explicitly who these entitled authorities shall be[36] nor how these authorities shall treat the data they receive[37]; but it makes (in para 1) a reference to the Police Act 578/2005, the Act on the Processing of Personal Data by the Border Guard 579/2005, the Customs Act 1466/1994 and the Coercive Measures Act 450/1987. The focal idea is, that Act 516/2004 regulates the retention of data, while the right to use the stored data shall be determined by other legislation. However, Sec. 14a on its part determines that the data in question may be only used for the purposes of investigating, solving and considering charges for criminal acts by the investigating authorities as referred to in Chapter 5a (3) (1) of the Coercive Measures Act 450/1987 (as described above).

The Coercive Measures Act 450/1987 rules general responsibilities of the police, the public prosecutor, the chief customs officials and the chief border guard officials. Chapter 4 – to which Sec. 14b (2) of Act 516/2004 makes a reference – regulates

---

32 The Act on the Openness of Government Activities 621/1999 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990621.pdf and in German at: http://www.finlex.fi/fi/laki/kaannokset/1999/de19990621.pdf

33 See Government Decree 503/2011 on the obligation to store certain data for the purposes of the authorities, of 12 May 2011 is available in Finnish at: http://www.finlex.fi/fi/laki/ajantasa/2011/20110503

34 See in this context the FiCoRA Regulation on the Obligation to Retain Identification Data, 53 A/2011 M, available in English at: http://www.ficora.fi/attachments/5z783w8Ue/Viestintavirasto53A2011MEnglanti.pdf

35 The Personal Data Act 523/1999 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf

36 See also answer 14 in the first questionnaire.

37 According to the explanations of the underlying Government Bill 158/2007 (available in Finnish at: http://www.finlex.fi/fi/esitykset/he/2007/20070158) para 4.2 the aim of the Bill was to improve the officials, particularly the police´s, scope and measures of operation.

different measures of seizure, namely Sec. 4b and 4c concerning the order to preserve data. Sec. 4b says that, if there is reason to believe, that data, which may be relevant for the clarification of the crime that is investigated, is lost or modified, the official who is entitled to arrest may impose an order to the party in possession or control of the data (but not the suspected) to preserve the data unchanged. This includes traffic data but excludes explicitly the respective content. According to Chapter 1 Sec. 6 of Act 450/1987 officials entitled to arrest are the police, the public prosecutor, the chief customs officials and the chief border guard officials. Sec. 4c rules that the one to whom the order of data preservation was addressed has to treat this order as confidential. An infringement of this secrecy obligation may be punished as secrecy offence or secrecy violation, according to Chapter 38 Sec. 1, 2 of the Criminal Code 39/188938. Regarding the officials handling of the received information, Chapter 4 Sec. 10 and 18 of Act 450/1987 have to be considered: the seized object must be maintained as such an be handled in a way that misuse is avoided; what is provided for the object also applies to the substance.

When the relevant data have been moved from the telecommunications company's area of responsibility to the one of the police (following the provisions of Sec. 36 of Act 516/2004 and Sec. 1, 36 of the Police Act 493/1995) the following provisions become relevant:

Sec. 18 of the Act on the Openness of Government Activities 621/1999 determines the authorities obligation to a good practice on information management, which refers inter alia to the secrecy and protection of documents, information management systems and the information contained therein. Sec. 24 of the Act 621/1999 specifies the official documents that have to be treated secretly, e.g. documents containing sensitive information on the private life of the suspect of an offence (para 24) and documents containing information on certain personal circumstances of a person (para 32). Sec. 36 gives the opportunity to issue more detailed decrees on the implementation of the act. Based on this Government Decree 681/201039 has been enacted. The Decree regulates the general requirements set to information security as well as to the classification of documents held by officials. It gives guidance to the establishing of good practices on the administration of information. Sec. 5 provides for the basic level information security shall achieve, particularly: to conduct a survey on possible information security risks, to ensure sufficient internal know-how on this subject, to determine tasks and responsibilities, to determine clearly who has which rights and to restrict access to the information held, to controle the fulfilment of the rules and to regularly assess the rules set. Chapter 3 includes the provisions on the classification of information, depending on their confidentiality and sensibility (protection levels I-IV). Following to this it is determined who may be entitled to have access to information of which protection level. Sec. 16 refers to electronic documents. It determines inter alia that documents

---

[38] The Criminal Code of Finland 39/1889 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf

[39] The Government Decree on Information Security in Administration 681/2010 is available in Finnish at: http://www.finlex.fi/fi/laki/ajantasa/2010/20100681

of protection levels I-II may be stored only on devices not connected to a communication network and strongly encrypted or otherwise strongly protected. Documents of other protection levels may be stored in a way connected to a communications network if the latter one is reliably protected against interruption. The officials have to implement the rules by 30 September 2013. Based on this Decree the Ministry of Finance (Valtiovarainministeriö) who is responsible for Information Security, has issued Guidelines40 on how to implement the information security provisions. These Guidelines are addressed to the management of organisations, their staff as well as to their persons in charge of operations, security, information services and information administration. Firstly, it stresses the importance of a sound planning, administration and comprehensive survey of the information held by the respective organisation as well as a solid analysis of risks. Staff concerned with the procession of data has to be guided, trained and controlled appropriately. Supervision, evaluation and obligations to report have to be carried out regularly. It has to be clearly decided and documented which personell shall have access to which information, to which scope and how. Communication networks and systems have to be created in a way that information security can be realised. The protection level of the networks and systems depends on the sensibility of the information concerned. There has to be a sound management and controle of rights to access (retraceable registration, identification and verification of entitled users, time limitation or other restrictions imposed on certain rightholders or on certain information) and of protection against malware or other disturbances. Depending on the protection level information shall be encrypted. Information the retention time of which has ended or which are not needed anymore shall be deleted/removed. The location/devices where information is stored shall be physically protected. Back up copies shall be made and the information strategy shall be developed further, on the grounds of the regularly conducted evaluations. Everyone having a certain right to access shall be supervised, the final responsibility is with the management of the organisation.

Chapter 7 (Information security and data storage) Sec. 32 of the Personal Data Act 523/199941 obliges the controller (of a register) to carry out the technical and organisational measures necessary for securing personal data against unauthorised access, against accidental or unlawful destruction, manipulation, disclosure and transfer and against other unlawful processing. Furthermore, the techniques available, the associated costs, the quality, quantity and age of the data, as well as the significance of the processing to the protection of privacy shall be taken into account when carrying out the measures. According to Sec. 3 (4) the controller is defined as a person, corporation, institution or foundation, or a number of them, for

---

40 The Guidelines (*Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta,* VM/2029/00.00.00/2010) of 19. October 2010 is available in Finnish at: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101028Ohjeti/02_Ohje_tietotuvallisuudesta_valtionhallinnossa.pdf

41 The Personal Data Act 523/1999 is availabe in English at: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf

the use of whom a personal data file is set up and who is entitled to determine the use of the file, or who has been designated as a controller by an Act.

The Act on the Processing of Personal Data by the Police 761/200342 provides in Sec. 13 for the police access to information from certain registers, inter alia concerning information from telecommunications operators, as laid down in Chapter 5a, Sec. 3 of the Coercive Measures Act, Sec. 31c of the Police Act and Sec. 35 and 36 of the Act on Data Protection in Electronic Communications (para 2 no. 5). Sec. 13 para 3 rules, that before data is supplied to the police with the aid of a technical interface, the police shall present an account of data security in the manner referred to in Sec. 32 of the Personal Data Act (see above).

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.

Sec. 14c of Act 516/2004 rules the following:

Statistics concerning the use of data to be retained for the purposes of the authorities
(1) The Ministry of the Interior shall provide the Commission of the European Communities on a yearly basis with statistics on using data retained by virtue of this Act. The statistics shall include:
1) the cases in which retained data was provided to the authorities;
2) the cases where the authorities' requests for retained data could not be met;
3) the time elapsed between the date on which the data were retained and the date on which the authorities requested for the data.
(2) The Ministry of the Interior shall in particular take the statistics referred to above in subsection 1 into account in its reports about telecommunications interception and monitoring to Parliamentary Ombudsman by virtue of the Police Act (493/1995), Coercive Measures Act or any other Act.

The annual reports on the secret investigation measures (named in Finnish: *Sisäasiainministeriön kertomukset eduskunnan oikeusasiamiehelle salaisten tiedonhankintakeinojen käytöstä*) according to Sec. 14c (2) are publicly available at: http://www.intermin.fi/intermin/home.nsf/pages/8783DF1E13178D8EC225705F0028C26E?opendocument.

The reports include information on telecommunication interception, telecommunication monitoring, the access to location data of mobile communication equipment and other rights of the police to obtain information, which refer to the rights according to Sec. 36 of the Police Act (see also Sec. 33 (3) of the Police Act, according to which the police has to inform the Ministry of Interior regularly on the secret investigation measures mentioned above) as well as to the Act 516/2004.

---

42 The Act on the Processing of Personal Data by the Police 761/2003 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/2003/en20030761.pdf

The 2010 report is available at: http://www.intermin.fi/intermin/images.nsf/files/e66e8be246b9ccd9c225785e0044fb9c/$file/kertomus_poliisin_tiedonhankinnasta_2010.pdf, it lists on page 19 under 2.4 the following figures:

In the year 2010 the police made use of its information rights addressed to telecommunications companies based on Sec. 36 (1) of the Police Act to 1153 connections; based on Sec. 36 (2) to 5116 connections and based on the Act 516/2004 to 746 connections.

The figures as to the year 2009 (available at: http://www.intermin.fi/intermin/images.nsf/files/b495c4a7432aa76ac22576f2004b400b/$file/kertomus_poliisin_tiedonhankinnasta_2009.pdf, page 15 under 2.4.) are: 1164, 5010 and 580.

Further information on these measures are not given, at least not in this public parts of the reports.

B. Country-specific questions

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

With a view to the research made in the legistaltion proceedings, inter alia by the responsible Parliamentary Committees, the relevant data retention provisions can be seen in conformity with the Finnish Constitution 731/1999[43] since its purpose is to protect public security and its intrusive measures can be assessed to be at an appropriate rate to the purposes. The content of confidential messages remain unaffected. The relevant aspects in detail:

Sec. 10 (1) of the Constitution protects everyone's right to privacy which includes the protection of personal data. Sec. 10 (2) protects the secrecy of correspondence, telephony and other confidential communications. According to Sec. 10 (3) these right are not absolute, but can be curtailed under certain conditions and circumstances, the enumeration of which in Sec. 10 (3) is to be seen as exhaustive. Any restrictions made to these rights have to be strictly limited and must not go further than necessary with regard to the concrete purpose.

The main intention of the constitutionally protected confidentiality of communication is to protect the confidential content of a message against outsiders. Besides this, it includes other information connected with the message which possibly can be relevant for its confidentiality, as for example a communication's

[43] The Finnish Constitution 731/1999 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf and in German at: http://www.finlex.fi/fi/laki/kaannokset/1999/de19990731.pdf

identification data[44]. However, according to the findings of the Constitutional Committee of the Parliament (*Perustuslakivaliokunta*) identification data do not belong to the core area of the constitutional protection of the secrecy of confidential messages[45]. Hence, not the qualified reservation of statutory powers of Sec. 10 (3) applies, but the general rules on the restriction of constitutional rights[46]. Hence, regulation concerning the processing of identification data may be issued on the level of an Act[47], as far as this meets the general requirements of restricting constitutionally protected rights.

The data retention provisions brought along a fundamental change from the prior to these existing needs of the telecommunications providers to retain identification data as far as necessary for their own purposes, to a retention obligation concerning the data of all of their users for a longer period and for the (potential) interests of the law enforcement authorities. According to the explanations of the underlying Government Bill HE 158/2007 the aim of the provisions is – corresponding with Art. 1 of the Directive – to ensure that certain information, which are connected to electronic communications and held by the telecommunications company, are retained for certain official purposes, particularly concerning serious criminal offences as specified by law. Thus, these restrictions can be seen as required by important public needs.

Furthermore, the data retention provisions do not require the storing of data *different* from those that had to be stored already before (see also the restriction in Sec. 14a (4) concerning the availability of the data), so in practice the changes may not become that noticeable, what is an important aspect as to the proportionality principle, an aspect that was criticised by the Data Protection Ombudsman. Moreover, the usage of the stored data and the authorities access to the stored data are permitted only in the cases determined by law on the level of an Act[48]. In order to minimise the intrusion into the constitutionally protected rights, it has been explicitly ruled by law, which legal principles apply when processing the respective data, how to provide for strict data security regulations and the obligation to determine the persons allowed to process data as well as how to supervise these efficiently.

With regard to the protection of privacy (Sec. 10 (1)) the legislator has made efforts to meet the constitutional requirements, too. According to the Constitutional Committee regulation on personal data, issued by an Act have to be comprehensive

---

44 See Government Bill 309/1993 proposing amendents to the fundamental rights of the constitution, available in Finnish at: http://www.finlex.fi/fi/esitykset/he/1993/19930309

45 See the opinion of the Constitutional Committee PeVL 9/2004, available in Finnish at: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/pevl_9_2004_p.shtml

46 See answer to question 51 of the first questionnaire.

47 See Government Bill 309/1993, as mentioned above.

48 See opinion of the Constitutional Committee PeVL 3/2008 upon Government Bill HE 158/2007, available in Finnish at: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/pevl_3_2008_p.shtml

and detailed[49], particularly with regard to the objective of the registration of the data, its content, the term of retention as well as the legal protection opportunities of the registered person. It is determined in the data retention provisions, who (Sec. 14a Act 516/2004, service providers obliged to submit a telecommunications notification) is obliged to store which data (Sec. 14 a Act 516/2004, identification data) as well as the duration of the retention (twelve months).

With regard to the latter one, HE 158/2007 explains that the term of 12 months (Sec. 14a (1) Act 516/2004) was the fair balance between the needs of the law enforcement authorities (to fulfil their duties within the meaning of the Directive) and the constitutional rights of the citizens (Sec. 10) and telecommunications companies (Sec. 15, see below). As the Constitutional Committee states, the risks going with data retention – regarding the secrecy of confidential messages as well as the protection of personal data – grow correspondingly to the duration of the storage. On the other hand a too narrowly considered time period may fail the retention purpose as a whole. Furthermore, the general principles of Act 516/2004 (Sec. 8) apply and it is clearly defined to which data the retention obligation applies, so that the general requirements of the restriction of constitutional rights, as certainty and defined limitation, are complied.

Sec. 15 of the Constitution provides for the protection of property. The data retention provisions oblige telecommunications companies to take certain measures in order to be able to fulfil the legal requirements, as for example to ensure sufficient storage space and data security and the acquirement of the needed or sufficiently powerful equipment. But since it is ruled that the costs for these measures are taken over by the official for the tasks of which the data are retained, this cannot be seen as unreasonable (see Sec. 14b (2) Act 516/2004 and Sec. 98 of the Communications Market Act 393/2003[50]).

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?

Yes, they are in parts. Sec. 10 (2) of the Constitution aims generally to protect the secrecy of confidential messages. The protection of the secrecy of confidential messages refers not only to the content of the message, but includes also other information attached to it which might be relevant for preserving its content confidential, as e.g. the identification data of a telephone call (see also the answer to question 7)[51].

As the Constitutional Committee has underlined in its opinion PeVL 9/2004 (see above) the main object of the secrecy of correspondence is to protect the

---

49 See opinion of the Constitutional Committee PeVL 51/2002, available in Finnish at: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/pevl_51_2002_p.shtml

50 The Communications Market Act 393/2003 is available in English at: http://www.finlex.fi/fi/laki/kaannokset/2003/en20030393.pdf

51 See explanations in HE 309/1993, available in Finnish at: http://www.finlex.fi/fi/esitykset/he/1993/19930309

confidentiality of the message's content. The identification data are regarded as not being part of the core area of the constitutional protection.

9. **As regards the answer to question 23 of the first questionnaire: how is it ensured in practice that data are not retained by more than one service provider (cf. Sec. 14b(1) of the Act)?**

   It is foreseen that – in the case that the authority detects the need to access data held by the service provider and notifies this need to the provider – the authority and service provider agree on how the official request should/could be accomplished. This is mainly in order to avoid high costs which have to be compensated by the authority (see below question 10). But this gives also the opportunity to decide beforehand who shall be obligated to retain which data. To avoid, that data are retained by more than one provider means, that e.g. in a case in which a message passes several telecommunications providers´ networks (which it usually does), it should – where possible – be tried to find in each communications event the service provider responsible to retain the data in question[52]. FiCoRA has issued a regulation prescribed in more detail which data shall be retained to meet the retention obligation as provided in Sec. 14a, 14b of Act 516/2004[53].

10. **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 used in the context of service provision, billing and related business activities?**

    Sec. 14b (2) 1 of Act 516/2004 refers to Sec. 98 of the Communications Market Act 393/2003 (see above) as to the compensation of the costs incurred by fulfilling the retention obligation. Sec. 98 (2) and (3) of Act 393/2003 – which is of great importance with a view to Sec. 15 of the Constituion – rule the following:

    > *(2) A telecommunications operator's right to receive a compensation from State funds applies only to the direct costs of the investment, use and maintenance of systems, equipment and software acquired to meet the needs notified by a public authority. The telecommunications operator's right to receive compensation from State funds also covers the direct costs incurred from any measures ordered by a public authority. Decisions on the compensation for costs incurred are made by the Finnish Communications Regulatory Authority.*
    > *(3) A telecommunications operator shall not use any systems, equipment or software funded by a public authority for its commercial activities.*

---

52 See explanations in HE 158/2007.

53 See Regulation FICORA 53 A/2011 M available in English at: http://www.ficora.fi/attachments/5z783w8Ue/Viestintavirasto53A2011MEnglanti.pdf

The "needs of the public authority" refer amongst others to the public duties of rescue and public safety authorities, pursuant to specific legislation, which particularly focus to information held by telecommunication providers. The services made to support the public authorities have to have efforded investments or work. These direct costs are for example espenses which arise from the planning of a software programm that has to be established for the collection of the required information, personnel expenses which arise from the use and maintenance of such a system or programme or the acquisition of technical equipment. These are not the costs of services provided for the (support/promotion of) the operators own activities or commercial offers. These are also not such services which – according ot special legislation – have to be free-of-charge. FiCoRA is the responsible authority do decide in a given case on the compensation. It decides whether and which costs are *direct* and therefore have to be refund and it decides on the amount of the compensation. On the coordination of decisions which technical equipment is refundable or not FiCoRA shall establish a working group (see also Sec. 96). Legal proceeding against such a decision can be made to the administrative courts[54]. The telecommunication operator´s invoice to the respective authority has to describe in detail on which particular service(s) it is based and deliver sufficient information in order to enable the authority to decide whether it is founded. However, the operator´s invoice is non-binding for FiCoRA. It should be noted that the law foresees – as a rule – that the authority clearly notifies its specific needs to the operator, hence, this notification can be used to assess which costs are actually refundable. This includes also, that the authority may instruct the operator which devices or measures should/could be chosen[55]. A clear notification should avoid controversies on the compensation already beforehand. The telecommunications operator shall fulfil these obligations as low-priced as possible and corresponding to the authority´s requests[56]. Ideally, the authority and the operator shall agree on the provision of information and the compensation of costs[57].

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

Neither the Coercive Measures Act nor the Police Act rule explicitly on such supervising. According to the Police Administration Act 110/1992[58] the Ministry of Interior is responsible for the guidance and supervision of the police. Underneath the Ministry but superior to the police divisions the Police Board (*Poliisihallitus*) acts as

---

54 See explanations in the Government Bill on amendments to the Communications Market Act HE 112/2002 (p. 175), available in Finnish at: http://www.edilex.fi/virallistieto/he/fi20020112.pdf

55 See also FiCoRA-decision 998/532/2006 of 31.10.2006, available in Finnish at: http://www.ficora.fi/attachments/suomimq/5kra6qlT0/PaatosSATPvsKRPkustannustenkorvaus.pdf

56 See Government Bill HE 112/2002, above.

57 See HE Government Bill 158/2007, above.

58 The Police Administration Act 110(1992 is available in Finnish at: http://www.finlex.fi/fi/laki/ajantasa/1992/19920110

the (central) Police Supreme Command. To the latter one Chapter 5a Sec. 15 of the Coercive Meaures Act makes a reference, concerning the measures of telecommunications interception and monitoring and technical surveillance. The provision rules that the Police Supreme Command supervises the conduction of these measures and determins the Ministry of Interior´s obligation to report to the parliamentary ombudsman annually (see above).

12. Clarifications regarding questionnaire I (German only):

Q16-19:

- **Ist der Zugriff auf Vorratsdaten für die Polizei tatsächlich nicht beschränkt auf die Ermittlung schwerer Straftaten? Sagt Chapter 5 a(3)(1) des Coercive Measures Act (450/1987), auf das in Art. 14a(1) e-Privacy Act verwiesen wird, etwas dazu? Kann auf die Daten für zivilrechtliche Verfahren zugegriffen werden? Trifft die Aussage "*The Act on the Processing of Personal Data in connection with the Enforcement of Punishment provides a number of grounds for the processing of personal data as well.*" (vgl. Antwort zu Q16) auch auf die gem. Sec. 14a e-Privacy Act gespeicherten Vorratsdaten zu?**

  § 14a (2) des Gesetzes 516/2004 bestimmt, dass die vorab genannten Daten nur zum Zwecke der Ermittlung, Klärung und zur Entscheidung über die Klageerhebung der in Kap. 5a § 3 (1) des Gesetzes 450/1987 (Coercive Measures Act) aufgezählten Straftaten verwendet werden dürfen. Der Katalog benennt nachfolgende Straftaten, wegen derer ein Verdacht bestehen muss:

  1) ein Verbrechen, dessen gesetzliche Höchststrafe mindestens vier Jahre ist;

  2) eine gegen ein System der automatischen Datenverwendung gerichtetes, unter Verwendung eines Telekommunikationsendgerätes begangenes Verbrechen, Zuhälterei, die Bedrohung einer in einem Rechtsverfahren anzuhörenden Person, eine rechtswidrige Bedrohung oder eine Betäubungsmittelstraftat;

  3) der strafbare Versuch eines der zuvor genannten Verbrechen;

  4) die Vorbereitung eines in terroristischer Absicht zu begehenden Verbrechens.

  5) ein schwerer Verstoß gegen die Vorschriften über die Zollerklärung;

  6) ein schwerer Fall der Verheimlichung illegalen Beutefangs; (betrifft Fälle der Wilderei, d.h. illegale Jagd und Fischfang).

  Kapitel 9 des Gesetzes 516/2004 bestimmt die Behörden, die Zugriff auf die Daten haben. Mit Blick auf § 36 dieses Gesetzes heißt es in den Erläuterungen des Gesetzentwurfs (HE 158/2007), dass andere Personen, als eben diese Behörden keinen Zugriff auf die nach § 14a zu speichernden Daten haben sollen.

  Das Genannte „*Act on the Prossessing of Personal Data in Connection ...*" 422/2002[59] befasst sich mit verschiedenen, im Zusammenhang mit dem

[59] Gesetz 422/2002 ist auf Finnisch abrufbar unter: http://www.finlex.fi/fi/laki/ajantasa/2002/20020422

Strafvollzug zu führenden Personenregistern bzw. sonst zu verarbeitenden personenbezogenen Daten. Eine Relevanz dieser Vorschriften für Vorratsdaten ist für mich nicht ersichtlich.

- **Gibt es einen Richtervorbehalt vor dem Abruf von Vorratsdaten? Wenn ja, wo ist dieser geregelt?**

  Nein, einen Richtervorbehalt explizit zum Abruf von Vorratsdaten gibt es nicht. Kap. 5a § 5 des Coercive Measures Act 450/1987 (Authorisation and decision; diese Vorschrift hat im Vergleich zum Stand der englischen Version erhebliche Änderungen erfahren) regelt jedoch die Entscheidungszuständigkeiten im Bereich der Telekommunikations- und technischen Überwachungs-/Ermittlungsmaßnahmen. Absatz 1 dieser Vorschrift bestimmt, dass über die in dem Kapitel beschriebenen Maßnahmen (TK-Abhören und –Überwachung nach Kap. 5a § 1; Ermittlung der Standortdaten von Mobilfunkgeräten (Kap. 5a § 3a); gegen einen Gefängnisinsassen gerichtete technische Abhör- und Beobachtungsmaßnahmen; technische Abhörmaßnahmen nach Kap. 5a § 4 und technische Abhör- und Beobachtungsmaßnahmen gegen einen Verdächtigen in dessen Fahrzeug oder Aufenthaltsort) auf schriftliche Anfrage des ermittelnden Beamten das nach Kap. 1 § 9 zuständige Gericht entscheidet. Absatz 2 geregelt, dass in eiligen Fällen der zuständige (*zur Festnahme berechtigte*) Ermittler über die TK-Überwachungsmaßnahme entscheiden kann. Der Antrag auf gerichtliche Entscheidung ist dann aber binnen 24 Stunden zu stellen. Absatz 3 erklärt, dass über andere technische Abhörmaßnahmen als die in Absatz 1 beschriebenen, in der Regel der Leiter der Ermittlungsabteilung (z.B. Leiter der Polizei-/Zoll-/Grenzschutzeinheit, zuständiger Staatsanwalt) entscheidet. In eiligen Fällen (so Absatz 4) darf abweichend von Absatz 3 der leitende Ermittler entscheiden, der aber dann wiederum binnen 24 Stunden die Entscheidung des Vorgesetzten (Absatz 3) einzuholen hat. Absatz 5 regelt schließlich, dass über andere als die in Absatz 1 genannten Fälle der technischen Beobachtung und Verfolgung der leitende Ermittler entscheidet.

- **Gibt es strafprozessuale Informationspflichten (z. B. im Coercive Measures Act) der abrufenden Behörden ggü. dem Betroffenen über die abgerufenen Vorratsdaten? Wenn ja, gelten diese Pflichten nur, wenn ein gerichtliches Strafverfahren eröffnet wird (also Anklage erhoben wird) oder auch, wenn das Ermittlungsverfahren eingestellt wird?**

  Das Coercive Measures Act enthält nachfolgende Informationspflichten gegenüber dem Betroffenen:

  Kap. 4 (Beschlagnahme von Gegenständen, Dokumenten und Daten) sieht in § 7 eine Informationspflicht gegenüber dem von der Beschlagnahme Betroffenen vor, sobald die Ermittlungen dadurch nicht mehr gefährdet werden.

  Kap. 5a (Abhören der Telekommunikation, Telekommunikationsüberwachung und technische Überwachung) sieht in § 11 (2) vor, dass der Betroffene, wenn die Ermittlungsergebnisse der Staatsanwaltschaft zugeleitet bzw. die Ermittlungen sonst abgeschlossen wurden, über die gegen ihn ergriffenen

verdeckten Maßnahmen informiert werden muss. Spätestens nach Ablauf eines Jahres muss der Betroffene informiert werden, auch wenn noch keine abschließende Entscheidung über die Ermittlungen getroffen wurde. Bei Vorliegen eines wichtigen Grundes kann das Gericht die zuletzt genannte Frist verlängern oder entscheiden, dass der Betroffene nicht informiert wird.

Eine vergleichbare Regelung explizit in Bezug auf Vorratsdaten gibt es nicht.

- **Sind die Regelungen zu Auskunftsrechten im Personal Data Act richtig beschrieben (Q18)?**

  Ja; eine englische Version des Gesetzes 523/1999 (Stand: 2001) ist abrufbar unter: http://www.finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf.

  Kap. 6 des Gesetzes 523/1999 regelt die Rechte des Registrierten. § 24 (1) sieht vor, dass der Inhaber des Registers dafür Sorge zu tragen hat, dass der Registrierte (in der beschriebenen Art und Weise) Information über die Verarbeitung seiner persönlichen Daten erlangen *kann*. § 24 (2) regelt Ausnahmen zu dieser Verpflichtung, die ebenfalls richtig beschrieben sind.

  § 25 sieht Informationspflichten über die Verarbeitung persönlicher Daten in besonderen Fällen vor; abweichend von der englischen Übersetzung gilt nur noch Absatz 3 der Vorschrift, der lautet:

  > *Where the name and contact information of an individual have been obtained from a personal data file for the purposes of direct marketing, distance selling or other direct advertising, or of market research or an opinion poll, or for a comparable addressed delivery, the file used, the controller and the address of the controller shall be mentioned. A teleseller shall give the same information upon request.*

  § 26 (1) bestimmt das Recht jedes Einzelnen, unbeschadet der Geheimhaltungsvorschriften zu erfahren ob/welche Daten von ihm in einem Register gespeichert sind. Die Absätze 2 und 3 beinhalten die beschriebenen Regelungen zu Kreditdaten.

  § 26 wird durch die Bestimmungen des § 27 beschränkt:

  > *Section 27 — Restrictions on the right of access*
  > *(1) There is no right of access, as referred to in section 26 above:*
  > *(1) if providing access to the data could compromise national security, defence or public order or security, or hinder the prevention or investigation of crime;*
  > *(2) if providing access to the data would cause serious danger to the health or treatment of the data subject or to the rights of someone else;*
  > *(3) if the data in the file are used solely for historical or scientific research or statistical purposes; or*
  > *(4) if the personal data in the file are used in the carrying out of monitoring or inspection functions and not providing access to the information is indispensable in order to safeguard an important economic interest or financing position of Finland or the European Union.*

(2) If only a part of the data on a data subject is such that it falls within the restriction on the right of access provided in paragraph (1), the data subject shall have the right of access to the remainder of the data.

Die allgemeinen Grundsätze für die Verarbeitung persönlicher Daten sind in Kapitel 2 des Gesetzes geregelt: Sorgfaltspflicht, Bestimmung des Verarbeitungszwecks, Zweckgebundenheit, allgemeine Voraussetzungen, Datenqualität und eine Beschreibung des Registers.

Q30: Bestehen für diesen Fall auch zivilrechtliche Schadensersatzansprüche?

Das Gesetz 516/2004 sieht selbst eine solche Bestimmung nicht vor. Bei Vorliegen der entsprechenden Voraussetzungen kommen Schadensersatzansprüche nach dem Tort Liability Act 412/1974 in Betracht[60].

Q33: Existieren Regeln über die Zusammenarbeit der abrufberechtigten Behörden untereinander und zwischen diesen und anderen Behörden über eine Weitergabe einmal abgerufener Vorratsdaten?

Das Gesetz 516/2004 enthält solche Regelungen nicht. § 35 des Police Act 493/1995 regelt das Recht der Polizei, von anderen Behörden Informationen zu bekommen. §§ 17 ff. des Act on the Processing of Personal Data by the Police 761/2003[61] regeln Zulässigkeit und Voraussetzungen für die Weitergabe bestimmter Daten, die die Polizei vorhält, an andere Polizeieinheiten bzw. an andere Behören.

Q35: Wie sind die Aufgabenbereiche von FICORA, Data Protection Ombudsman und Parliamentary Ombudsman im Kontext der VDS abzugrenzen?

Regelungen hierzu enthält Kap. 8 des Gesetzes 516/2004[62] (Guidance and Supervision). § 31 bestimmt die Aufgaben der FiCoRA, u.a. die Überwachung der Einhaltung der Vorschriften des Gesetzes 516/2004 und der darauf basierenden weiteren Bestimmungen, sofern nicht § 32 etwas anderes bestimmt. § 32 bestimmt seinerseits die Aufgaben des Data Protection Ombudsman, die sich demnach aber nicht auf die VDS erstrecken. Der Parlamentarische Ombudsmann hat generell die Aufgabe, das Handeln der öffentlichen Stellen sowie speziell, die TK-bezogenen und/oder heimlichen Ermittlungsmaßnahmen zu überwachen[63].

---

60 Das Gesetz 412/1974 ist auf Englisch abrufbar unter: http://www.finlex.fi/fi/laki/kaannokset/1974/en19740412.pdf

61 Gesetz 761/2003 ist auf Englisch abrufbar unter: http://www.finlex.fi/fi/laki/kaannokset/2003/en20030761.pdf

62 Gesetz 516/2004 ist auf Englisch abrufbar unter: http://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf

63 Informationen finden sich auf Deutsch und Englisch unter: http://www.oikeusasiamies.fi/Resource.phx/eoa/english/de/index.htx.

Q40/42/43 (inkl. Fußnoten/Kommentare): Sind die genannten Guidelines etc. auf die VDS anwendbar, und welche Regeln enthalten sie insoweit (hinsichtlich der auf Englisch verfügbaren Texte genügt ein Hinweis auf die jeweilige Vorschrift)?

Q42: auf der angegebenen Seite www.tietoturvaopas.fi sind die genannten Guidelines nicht zu finden. Die Principles and Good Practices (vm 37/01/2006)[64] richten sich an den beschriebenen Adressatenkreis. Ziel ist im Wesentlichen, dass jede Organisation für die von ihr geführten Datensysteme und Personenregister bestimmen soll, welche Personen zur Nutzung dieser berechtigt sind, den Inhalt dieser Nutzungsrechte sowie deren Beendigung. Das Finanzministerium (*Valtiovarainministeriö*) ist sachlich zuständig für die Leitung und Entwicklung der Datensicherheit der staatlichen Verwaltung. Die Erkenntnisse der eigens hierfür eingerichteten Arbeitsgruppe VAHTI sollen auch der kommunalen Verwaltung, dem Privatsektor, der internationalen Zusammenarbeit und dem Handeln der Bürger zugute kommen. Der Schwerpunkt der Betrachtungen liegt auf Organisationen, die große Datensysteme nutzen. Behandelt wird die interne Verwaltung von Daten. Nicht Bestandteil der Betrachtungen ist die Überlassung von Daten an Personen/Einrichtungen außerhalb der betreffenden Organisation (die Grenzen der Organisation überschreitenden Weitergabe der Daten). Verantwortlich ist die Führung der jeweiligen Organisation. Hinsichtlich der erforderlichen Verfolgung einer Datensicherheitspolitik verweist das Dokument auf den Sicherheitsstandard ISO 17799 (heute: ISO 27000)[65]. Darüber hinaus weist das Dokument darauf hin, dass am Beginn jeder Implementierung eines Datensicherheitsprogramms eine fundierte Risikoanalyse zu erfolgen hat, die die Grundlage späterer Maßnahmen sein soll. Die Risikoanalyse sollte regelmäßig wiederholt werden[66].

In particular: do they provide for measures in one or more of the following areas:

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

It is foreseen, that certain data (depending on their classification of confidentiality, see below) can be used only within systems that are not connected to a larger / any network.

- 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)

---

64 Auf Finnisch unter: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061122Kaeyttoe/vahti_9_06.pdf

65 ISO 27000 ist auf Englisch abrufbar unter: http://www.17799central.com/.

66 Vgl. zu diesem Thema auch die Antwort in Frage 5, oben.

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

All data/data administration systems must be in the clear responsibility of a certain "owner" (unit the data belong to). This owner decides how to fulfil the requirements established by the risk analysis, decides who shall/shall not be entitled to use which data for which purposes, supervises and evaluates regularly all measures in this field. The rights to use data are not convincingly to be granted on an individual basis but referring to certain "roles" within the organisation. The register of the staff and the "whether and how" of their rights to use data is to be seen as the core of the data administration system and has therefore to be kept up-to-date. Certain technical aspects may be delegated to the IT-unit of the organisatioin but the general responsibility stays with the owner.

All data has to be classified according to their degree of confidentiality. Furthermore it may be ruled that the right to use certain data (depending on their classification of confidentiality) is restricted to certain times or situations or maximum duration.

The right to access data shall end immediately and comprehensively after the employment of the responsible staff ends or its area of deployment changes.

- access logging

It is foreseen, that certain data (depending on their classification of confidentiality, see below) can be accessed by a "strong identification" of the respective user, only. Access control can be realised by time-recording systems and a reliable system identification and verification of the user (reference is made to SAML-stabdard).

- secure (irreversible) deletion after expiry

Data that are not needed anymore or to which a definite retention time was set have to be deleted in a way that data protection and security are ensured. The owner shall set a retention time according to the provisions of the Archives Act 831/1994[67].

- 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

---

[67] The Archives Act 831/1994 is available in Finnish at: http://www.finlex.fi/fi/laki/ajantasa/1994/19940831?search%5Btype%5D=pika&search%5Bpika%5D=arkistolaki

All decisions made / measures taken / rights given have to be documented in a way which ensures that these can be reconstructed. It is suggested to conduct regularly – at least once a year – a review and / to implement a system of regular reporting on the compliance with the data security rules set, that the documents on the given rights/entitled persons are uptodate and that relevant changes or new rules are considered as well as the removal of unnecessary/unused rights. Each register shall also have a description which clearly defines the purpose which data are stored / may be used for.

- 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)

When the owner decides on the granting of rights to certain persons/roles the principle of necessity has to be considered. On this principle it shall be decided whether and to which scope rights to use data shall be granted. Rights that have become or have shown to be redundent shall be removed.

The registered person shall be entitled to receive information on which data are in the reigister as well as the correction of incorrect data.