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

Sweden

Christine Kirchberger

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?

No, the Directive has not yet been transposed into Swedish law. A Governmental Official Report was published in 2007 (see below), which eventually lead to the recent government bill. The Government Bill (Prop. 2010/11:46) was, however, postponed in the Swedish Parliament, and a decision is not to be expected before May 2012.

- ***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)?

The reasons for non-transposition are several fold, and include a change in political power after parliamentary elections in 2006 from social democratic to the conservative block (the conservatives seeing more privacy issues than the former government); difficulties in agreeing on sharing of costs by stakeholders, and parliamentary elections in 2010 which slowed down the legislative process one more time.

After the judgement by the European Court of Justice in February 2010 (C-185/09), the Swedish government planned to submit a government bill, but decided later to await the elections in autumn 2010 until a final proposal is being submitted to the parliament for voting. This proposal was presented in October 2010, Governmental Bill 2010/11:46 (*Prop. 2010/11:46 - Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG*). The Bill was, however, not accepted by the majority of the parliament and a new vote cannot be accepted before March 2012.

In general, data retention has been very much discussed in the Swedish media, not only on a broad level but also specifically by communication service providers with regards to the possible costs involved in the storing of data. The question of who will carry the costs for data retention has apparently been one of the major obstacles to the legislative process. In addition, different political ambitions play an important role, as the governing parties do not have a clear majority at the moment.

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?

A Governmental Official Report, which commonly precedes any legislative bill in Sweden, was presented in 2007 (SOU 2007:76 - Lagring av trafikuppgifter för brottsbekämpning).

A Governmental Bill (*Prop. 2010/11:46 - Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG*) was subsequently submitted to the parliament in November 2010, where it was referred to the Committee for Legal Affairs (*Justitieutskott*). The Bill was finally debated and voted upon by the Parliament in March 2011, where it was decided that the draft law should be referred back to the Committee for Legal Affairs for at least another year.

A new vote can, therefore, earliest be expected in March 2012.

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.**

Legislative process

The Governmental Official Report SOU 2007:76 *Lagring av trafikuppgifter för brottsbekämpning* (available in Swedish at http://www.sweden.gov.se/content/1/c6/09/15/21/2f8c7424.pdf) was published in 2007 and contains a preliminary draft for a legislative bill stipulating amendments to the Swedish Electronic Communications Act (*Lag (2003:389) om elektronisk kommunikation*, available in Swedish at https://lagen.nu/2003:389) as well as a new Regulation on data retention. (Question 7) The report is only available in Swedish at the moment. (Question 5)

The Governmental Report was followed in November 2010 by a Government Bill (*Prop. 2010/11:46 - Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG*). The Bill is available in Swedish at http://www.sweden.gov.se/sb/d/13654/a/157433.

The changes in the Bill compared to the Official Report mainly concern the legislative technique of the implementation,

In order to guarantee a more technological neutral regulation, the Government suggests to stipulate the different types of information to be retained as well as the purpose of the retention in a statute, while more technological descriptions of what can be retained should be dealt with in an Ordinance in order to be able to adapt to the technological development. The necessary changes on a statute level are to be implemented in the Swedish Electronic Communications Act (Lag (2003:389) om elektronisk kommunikation).

This approach is in line with general efforts to keep legislation rather technology neutral and regulate specific details in Ordinances and administrative provisions. An example for this is the electronic tax declaration, where the relevant Act only stipulates the possibility of submitting one's declaration electronically, whereas the appropriate Tax Authority Regulation states the necessary technical requirements, such as which eID to use.

Definitions (Question 8)

Whereas the Directive has a more vertical approach to the different areas to be included in data retention, the Swedish proposal aims at a more horizontal approach. As different sectors start to overlap with each other due to developments in technology, the proposed regulation focuses on a more neutral way to structure the different areas.

The Government Bill, therefore, suggests that the following four technical areas should be encompassed by data retention regulations (the areas were already mentioned in the Official Report from 2007):

- Telephony (electronic communication service that allows the possibility to call or receive calls via one or several numbers within a national or international numbering plan)
- Messaging (exchange or transfer of electronic messages, which are not conversations, or information, which is transmitted as part of a radio or TV programme. This definition may be slightly different to the one chosen in the Directive)
- Internet access (the possibility to transmit IP packages which give the user access to the Internet)
- Type of connection (the capacity which is offered to get Internet access; this area is not specifically mentioned in the Directive)

Different to the Governmental Official Report, the Bill proposes that the Act only stipulates an obligation to retain the data, whereas the specific details of the obligation should be regulated in an Ordinance. In other words, the Act would regulate which technology areas it applies to, though not any definitions of these, and the legislative aims with the retention, such as to identify and track a source of communication. The exact list of what information should be retained and the relevant definitions are to be regulated in an Ordinance.

Information to be retained

The information to be retained shall identify or track the source of communication, destination of communication, date, time and length of the communication, type, equipment and localisation of mobile equipment at the communication's start and end. As mentioned above, the Bill does not contain any further definitions or lists of data, as these are to be dealt with in the according Ordinance.

The content of messages (including IP packages) does not fall within data retention (in accordance with Article 5 (2) Directive). IP addresses as such, however, are to be stored in accordance with the Directive.

Periods of retention (Question 13)

While the Official Report from 2007 suggested one year as the period of retention, the Government Bill proposes 6 months. Data that has not been requested by the crime fighting authorities within 6 months is to be destroyed.

Question 9

The proposed amendments in the Government Bill suggest retention of localisation data and data about unsuccessful call attempts, and reaches, in this respect further than the Directive. Article 3 of the Directive leaves it up to the Member States to decide if data concerning unsuccessful call attempts, which was only generated and processed, and not necessarily stored or logged, should be retained. As the Swedish

crime fighting authorities expressed a need for access to information about unsuccessful call attempts, the Government proposes to introduce an obligation to retain data in these cases. As the obligation in Article 3 only concerns data that is stored or logged, the Swedish proposal reaches further than the Directive, as it also concerns data, which is only generated or processed. Such an obligation is, however, in accordance with Article 15 (1) of the Directive on Privacy and Electronic Communication (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector).

Regarding localisation data for mobile communications equipment, the Swedish Government uses the term *localisation information* instead of *Cell ID* mentioned in the Directive.

In addition, the Directive does not stipulate any obligation to retain localisation data at the end of a communication. As, even in this case, the crime fighting authorities expressed a need for this type of information, the Government Bill proposes such an obligation in accordance with Article 15 (1) of the Directive on Privacy and Electronic Communication.

Though an expressed wish by the crime fighting authorities to even be able to access localisation data during a communication, the Swedish Government considered such a request as invading the privacy too much as well as leading to even higher costs.

The new amendments do not include any obligation for communication providers to collect any information, but solely to retain already collected data. This is in accordance with the Swedish interpretation of Article 3 in the Directive, mentioned in the Official Report as well as the Government Bill. Communication providers, in other words, only have to retain traffic data that was generated or processed in their own systems.

Questions 10 and 12

The Swedish Electronic Communications Act already today allows for the storage of certain traffic data, but only under specific circumstances mentioned below. In other words, retention of data is the exception, deletion the norm. (Question 10 and 12)

The current in force Chapter 6 Section 5 Swedish Electronic Communications Act stipulates an obligation for network operators to erase or anonymise traffic data, such as telephone number/IP address of the sender and receiver, and the date and time of a communication. Electronic communication providers are only allowed to process such data as long as it is necessary for the transmission of the message. In addition, billing purposes and the consent of the subscriber are acknowledged reasons for processing, for a certain period of time at least. Location data, which is not traffic data, may only be processed with regards to value added services. (Question 10 and 12)

The governmental report considered it technically impossible and not reasonable to create a system that exempts retention of data of certain people who can be released

from the duty to testify (in accordance with Chapter 35 Section 5 Swedish Code of Judicial Procedure). Swedish law does not stipulate any general lawyer-client privilege as such, the only exception being communications between the suspect and his/her attorney (according to Chapter 27 Section 22 Code of Judicial Procedure). Coercive measures can therefore be decided by the court regarding doctors, priests, journalists, etc. to the extent the measure is considered proportional to its purpose, such as e.g. secret wiretapping. As the Code of Judicial Procedure allows surveillance of the content of communications (with the exception of suspect-attorney communications stated above), it is not likely that the provisions regarding release of traffic data by service providers will be stricter in this respect.

Access to data

Access to data as such is not dealt with in the current Government Bill. The Swedish Government has, however, investigated crime fighting authorities' access to electronic communication data for a few years. Several Governmental Official Reports on access have been published since 2005, e.g. SOU 2005:38 (Tillgång till elektronisk kommunikation i brottsutredningar m.m.) and SOU 2009:1 (En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen). No Government Bill has, however, been presented yet in this regard.

The latest report suggests, however, the enactment of a new statute concerning access of authorities to data on electronic communications (Förslaget till lag om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet). The suggested new Act should allow access to data in order to prevent and detect criminal offences, which could lead to imprisonment for at least two years. These reports do not specifically refer to the Data Retention Directive and do not seem, therefore, to aim at transposing the Directive.

Crime fighting authorities commonly include the National Police Board (NPB – *Rikspolisstyrelsen*), the police, prosecutors and other public authority involved in crime intervention, such as Swedish Customs and Costal Guard. Different Acts or Ordinances, such as the Ordinance 2008:1396 on simplifying the exchange of information and intelligence between law enforcement authorities in the European Union, may define the term more detailed, but there is no general definition of the term otherwise. Ordinance 2008:1396 transposes Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

According to the currently in force rules, they can access the data either via a court order for secret wiretapping (*hemlig teleavlyssning*) or surveillance (*hemlig teleövervakning*) according to Chapter 27 Section 18 or 19 Swedish Code of Judicial Procedure (*Rättegångsbalk (1942:740)*). The first possibility (secret wiretapping) requires a court order and includes information on the content of a communication; the second possibility (secret surveillance) has lower requirements, though a court

order is still required, but only grants access to historical data about the subscription and traffic data. (Question 14, 15, 16 and 17)

Secret wiretapping is at the moment only allowed for crimes that could lead to imprisonment of at least 2 years (Chapter 27 Section 18 Code of Judicial Procedure. Secret surveillance requires that the investigation concerns a crime, which could lead to imprisonment of at least 6 months, or specific other crimes mentioned in Chapter 27 Section 19 Code of Judicial Procedure (e.g. data intrusion, narcotic trade, smuggling, etc.).

In addition, crime-fighting authorities can access traffic and subscription data according to the Electronic Communications Act. Chapter 6 Section 22 Para 1 point 2 allows the public prosecutor, the police or another authority that is investigating a crime, access to information about a subscription, such as name, address, subscription number (e.g. phone number, IP number). The provision, however, requires that the investigated crime could lead to imprisonment.

Chapter 6 Section 22 Para 1 point 3 allows the same authorities to access data that is generated when a communication takes place, traffic data in other words. The requirement in this case is investigation of a crime that could lead to imprisonment of at least 2 years. In both cases of access according to the Electronic Communications Act no court order is necessary, but the request for access comes directly from the police, prosecutor or other crime fighting authority.

With the transposition of the Enforcement Directive (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights), private entities received the right to seek an 'order to provide information' (*informationsföreläggande*) before the Court according to Article 53c Swedish Copyright Act (*Lag (1960:729) om upphovsrätt till litterära och konstnärliga verk*). Communication providers can, therefore, now be forced to release personal data about their subscribers if this information is still stored in their systems. (See more below under Question 45)

The suggested amendment does not mention any notification of the aggrieved party, but Section 26 Swedish Personal Data Act (*Personuppgiftslag (1998:204))* stipulates a general right for the individual to request information about what data is stored about her/him. The Personal Data Act is, however, subsidiary to any other legislation. Regarding wiretapping and surveillance, Chapter 27 Section 31 Code of Judicial Procedure stipulates an obligation to inform the suspect of the surveillance as soon as there is no risk for the investigation anymore. (Question 18)

Neither the report nor the Bill suggest any amendments with regards to the already existing provisions concerning civil and criminal liability. The general principle of confidentiality of communications, stipulated in Chapter 6 Section 20 Electronic Communications Act, protects all data kept by electronic communication providers. Breaches of confidentiality can lead to civil liability (Chapter 6 Section 2 Electronic Communications Act refers to the Swedish Personal Data Act) and/or criminal liability (Chapter 7 Electronic Communications Act). In addition, Chapter 20 Section 3 Swedish Penal Code (*Brottsbalk (1962:700)*) punishes breach of

professional confidentiality with a fine or imprisonment for at most one year. (Question 20 and 21)

The Government Bill does not suggest any specific provisions on failure of providers to fulfil their retention obligations. The Electronic Communications Act does, however, include some general legal remedies for the supervisory authority (PTS) to control the legislation being followed. These remedies are mentioned in Chapter 7 of the Act and include fines and injunctions.

The crime fighting authorities receiving the data have to meet the requirements of the special legislation governing databases kept by various Swedish authorities. See further Q46.

Security (Question 21/26)

The Government Bill, as the Governmental Official Report from 2007, underline the importance of safeguarding that retained data is not used or spread unauthorised, in accordance with Article 7 of the Directive. The Bill suggests the introduction of a specific obligation for communication providers to take the necessary technical and organisational measures to secure processing of retained data. This obligation is stipulated in the new Chapter 6 Section 3a of the Electronic Communications Act. The Section further mentions that the Government or the supervisory authority should deal with the specifics of this obligation in authority regulations.

Possible measures, according to the Report form 2007, could include only authorised personal having access to the data and the data being stored in different systems than the everyday ones.

Providers to fall under the data retention obligation (Q 23/24)

The governmental report suggests that all electronic communication providers who have to register their services with the Swedish supervisory authority, Swedish Post and Telecom Agency (PTS), will fall under the obligation to retain data. These organisations are those which provide a public communications network that is generally provided for a fee or which provide publicly available communication services. Services that are only offered to a closed group are exempted, e.g. internal company networks. More information at PTSs website (http://www.pts.se/en-gb/Industry/Telephony/Anmalningsplikt-operatorer/)

Question 25

Regular traffic data can already today be retained for billing purposes (see above)

Costs

The governmental report mentions some estimates on the possible costs for the service providers and suggests around 100 million Swedish crowns (ca 10 million Euro) in order to identify and save the data, and another 100 million Swedish crowns to retain the data if every provider stores the data in their own system.

(Question 27). The report suggests that the data should be stored at the premises of each provider and not in a central system of any kind. The costs for releasing the data upon request are estimated to around 20 million crowns (ca 2 million Euro).

The question of sharing of costs and reimbursement for service providers by the state has been discussed in the media to a large extent and though the report suggests that service providers carry the costs and should be reimbursed when they release the data to the crime fighting authorities, several other opinions have been shared since then, so the answer to this question remains to be seen.

Question 29.

The current in force legislation governing access to data held by communications providers is the Electronic Communications Act, in particular Chapter 6. In addition, the already mentioned rules in the Code of Judicial Procedure apply.

Question 30

Chapter 6 Section 2 Electronic Communications Act refers to the Personal Data Act for possible sanctions. In particular, questions of civil liability are to be answered according to the Personal Data Act. According to Section 48 Personal Data Act an individual shall be compensated for damages caused by unlawful processing of personal data.

Chapter 7 Electronic Communications Act contains provisions on criminal liability for, inter alia, breach of confidentiality. Section 15 stipulates that breach of confidentiality can lead to fines. Breach of confidentiality can also lead to criminal liability according to the Swedish Penal Act.

Question 31

According to the legislation currently in force, access to subscription or traffic data according to the Electronic Communications Act is requested by the crime fighting authority that needs the data; see further Chapter 6 Section 22 of the Act. In other words, there is no specific public body that particularly is responsible for establishing the contact with the provider.

Question 32

To the extent local or regional authorities have crime fighting functions, they can fall within Chapter 6 Section 22. Commonly, the crime fighting authorities include the police, public prosecutor, the Swedish Economic Crime Authority (*Ekobrottsmyndigheten*), Swedish Customs (*Tullverket*), Coast Guard (*Kustbevakning*) and the Swedish Tax Authority (*Skatteverket*).

Question 33 and 34

There is no specific Act governing co-operation among the different bodies, except the general rules of the Electronic Communications Act.

The Swedish Government Bill on data retention explicitly mentions, that the term crime fighting authorities in the Acts does not include non-Swedish authorities. The Bill does not further discuss the issue. When it comes to exchange of data in general with other EU Member States, Ordinance 2008:1396 on simplifying the exchange of information and intelligence between law enforcement authorities in the European Union transposed Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union.

Commonly, the public prosecutor or the court provide legal help to foreign authorities, in accordance with the International Legal Assistance in Criminal Matters Act (lag (2000:562) om internationell rättslig hjälp i brottmål, a somewhat out-dated version in English is available at http://www.sweden.gov.se/sb/d/3926/a/27769)

Supervisory authority (Q 35)

As is the case for electronic communications in general, the Swedish Post and Telecom Agency (PTS) (http://www.pts.se/) will be the responsible supervisory authority with regards to data retention. PTS is an independent agency, it reports to the Ministry of Industry, Employment and Communications, and is managed by a board appointed by the Government.

To the extent the retained data is considered personal data, the Swedish Data Inspection Board (*Datainspektionen*) is also responsible in its supervisory function for data protection. In this regard, both authorities have overlapping supervisory power.

- ***If transposition has been accomplished:***

General questions

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

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

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

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

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

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?**

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?**

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.**

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

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)?**

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.**

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)?**

15. **For which purposes may the data retained be used according to the national law transposing the Directive, for which purposes may they be used according to other national law (e.g. for law enforcement (criminal/administrative**

offences), security, civil action (e.g. to enforce copyright claims))? Does the national law grant any rights to individuals to access the data retained directly, e.g. in a civil action (right to information on the owner of an IP address)?

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

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?**

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?**

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

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

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.**

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

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.**

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?**

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?**

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)?

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)?**

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?**

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

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.**

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?**

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?**

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?**

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)?**

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)?

II. Relevant case-law

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

No, as the Directive has not been transposed yet.

If so, please answer to the following questions:

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

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

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

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

The European Court of Justice ruled on 4 February 2010 that Sweden failed to adopt, within the prescribed period, the provisions necessary to comply with the Directive (Case C-185/09, *European Commission v Kingdom of Sweden*, Judgment of the Court of 4 February 2010).

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?

At the moment, service providers store the data at their own premises or at least under their own responsibility. According to the Governmental Official Report it does not seem that there will be any changes in this respect.

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?

N.A., as the Directive has not been transposed yet.

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

a) no data are retained beyond what is permitted?

N.A., as the Directive has not been transposed yet.

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)?

N.A., as the Directive has not been transposed yet.

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

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.

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

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)?

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

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)?

N.A., as the Directive has not been transposed yet.

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?

N.A., as the Directive has not been transposed yet.

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.

N.A., as the Directive has not been transposed yet.

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?

N.A., as the Directive has not been transposed yet.

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 topic has been lively discussed for several years, both in the public media and in the political arena. While the original enactment of the Directive was actively driven by the former Swedish Minister of Justice (from the Social Democrats), the now in power government (conservative block) has been more hesitant to transpose of the Directive.

Communication providers have been criticising the draft legislative proposal mainly due to questions of privacy concerns and the possible costs connected with the data retention. In the light of the enactment of the Enforcement Directive, several electronic communication providers even chose to delete personal data, referring to the right to privacy and their duty of confidentiality. Several court cases have been initiated in this regard (Telia Sonera, one of the largest communication providers in Sweden, and ePhone, an Internet service provider, being the two main cases) and the Swedish Supreme Court recently referred the ePhone case to the European Court of Justice for a preliminary ruling in order to receive clarification to the relation between the Data Retention Directive and the right to information according to the Enforcement Directive.

The ePhone case started when five book publishers requested ePhone, a Swedish provider of electronic communication services, to release information about IP numbers of its customers. The provider refused and was sued by the publishers. The district court ordered the data to be released, while the Appellate Court (*Hovrätt*) was of another opinion. According to the *Hovrätt* the audiobooks required login information and the plaintiffs had not done any investigation into the making available of the login information. For these two reasons the Appellate Court decided that there was no probable cause that the audiobooks were made available to the public and therefore infringed copyright. As a consequence the requirements for an 'order to provide information' (informationsföreläggande) according to Article 53c Swedish Copyright Act were not fulfilled, and ePhone did not have to provide the publishers with information about its customers.

New legislation in 2008 concerning the right of the Swedish signal intelligence agency, FRA, (the National Defence Radio Establishment) to eavesdrop on all Internet, telephone and fax traffic shifted the focus in the public debate from data retention to surveillance in general. (See more on the blog post from several colleagues from Stockholm University http://klamberg.blogspot.com/2008/10/fra-law-sleepwalking-into-surveillance.html and at EDRI http://www.edri.org/edrigram/number6.21/fra-surveillance-society.)

The Swedish Post and Telecom Agency keeps an updated website dedicated to the transposing of the Directive (http://www.pts.se/sv/Bransch/Internet/Integritet/Regler/Trafikdatalagring/).

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)?

Not in particular. The processing of personal data by private entities and organisations is regulated in the Swedish Personal Data Act while data processing by public authorities mainly is governed by specific statutes, such as the Police Data Act (*Polisdatalag (2010:361)*), the Patient Data Act (*Patientdatalag (2008:355)*), the Act on the National Address Register (*Lag (1998:527) om det statliga personadressregistret (SPAR)*), and the Act on Processing of Data by the Tax Agency for Taxation Purposes (*Lag (2001:181) om behandling av uppgifter i Skatteverkets beskattningsverksamhet*), to mention a few.

These Acts stipulate very specifically the conditions under which authorities are permitted to store and retain personal data with regards to the databases kept by them. The Police Data Act, e.g., contains specific provisions on the conditions under which personal data may be processed by the police authorities. In other words, processing and retaining of personal data is very much regulated in Sweden and generally not allowed without any specific reason.

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.

Though the Governmental Official Report underlined the importance of statistics with regards to the use of data retention, no such statistics have been collected yet. To some extent, the Swedish police and Prosecution Authority have been collecting data in this regard, in their annual report to the government concerning the amount of court orders for secret wiretapping as well as the crime that gave rise to the order. In their latest report (*Skr. 2009/10:66 Hemlig teleavlyssning, hemlig teleövervakning och hemlig kameraövervakning vid förundersökning i brottmål under år 2008*) the amount of granted orders for secret wiretapping according to the Code of Judicial Procedure in 2008 reached 990.

A Swedish Governmental Official Report in 2005 (*SOU 2005:38 - Tillgång till elektronisk kommunikation i brottsutredningar m.m.*) estimated the amount of requests to release data according to the Electronic Communications Act to 4000 per year.

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?

N.A., due to non-transposition of the Directive.

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?

No, due to non-transposition of the Directive.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications:

Which data are – according to national (constitutional) law1 – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

The Swedish constitution consists of four separate statutes, including the Instrument of Government (*Regeringsform (1974:152)*). (For more information see http://www.riksdagen.se/templates/R_Page____6307.aspx.) The Instrument of Government stipulates in Chapter 1 Article 2 that the public institutions shall protect the private and family lives of private people.

Chapter 2 Article 3 Paragraph 2 mentions more specifically privacy with regards to data processing:

> Every citizen shall be protected, to the extent set out in more detail in law, against any violation of personal integrity resulting from the registration of personal information by means of automatic data processing.

According to Chapter 2 Article 22 point 2 foreign nationals are also protected against violations of privacy.

In addition, Chapter 2 Article 6 safeguards privacy with regards to correspondence, eavesdropping, the recording of telephone conversations and other confidential communications.

The European Convention for the Protection of Human Rights and Fundamental Freedoms is guaranteed in the Swedish constitution through Chapter 2 Article 23 Instrument of Government.

The recent changes of the Instrument of Government mainly concerned the Swedish membership in the European Union and several other procedural roles of voting. Concerning personal integrity, Chapter 2 Article 6 was amended and now includes an additional general protection against invasions of personal privacy:

"In addition to what is laid down in paragraph one, everyone shall be protected in their relations with the public institutions against significant invasions of their personal privacy, if these occur without their consent and involve the surveillance or systematic monitoring of the individual's personal circumstances." (See original text at http://www.riksdagen.se/templates/R_PageExtended____6319.aspx)

---

[1] 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).

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?

According to Chapter 2 Article 12 Instrument of Government restrictions may be applied to satisfy a purpose acceptable in a democratic society. The restriction may, however, not go beyond what is necessary with regards to the purpose, which occasioned it.

With respect to protection of privacy, there are four general principles that come into play concerning coercive measures. These principles concern legality, purpose, assessment of need and proportionality.

The principle of assessment of need stipulates that a coercive measure should not be applied if it is not necessary for the purpose of the measure and a less intrusive measure is sufficient. The principle of proportionality states that type, extent and duration of the coercive measure should be in adequate relation to the purpose and reason for the measure.

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?

No, as the Directive has not been transposed yet.

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

As most fundamental rights, the right to privacy is not an absolute right but has to be balanced against other accepted interests in society. Crime fighting purposes, typically, constitute such other interests.

Swedish constitutional law does, in other words, not stipulate an absolute limit to surveillance measures, but requires a balance of interest to be carried out. This balance is reflected in the Government Bill on data retention as well, as the interests of crime fighting authorities and the privacy of individuals are discussed.

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)?

As Swedish national law does not stipulate any general lawyer-client privilege, no such obligation can be found in the constitution either.

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?

No such discussions have taken place.

Already in 1996 a duty for communication providers was introduced (*anpassningsskyldigheten*) to manage their operations in a way that allows decisions on secret wiretapping and surveillance. This obligation was implemented in order to facilitate crime-fighting authorities' access to data held by the providers.

In line with the privatisation of previously state-owned telecommunication providers the Government saw a risk of the cooperation between providers and the police not fully functioning. It is, furthermore, not technically feasible that the crime fighting authorities build up systems that allow storage of all this data. In this regard, the communications providers are the only ones who have the possibility to store the data in question.

The obligation to adapt is currently stipulated in Chapter 6 Section 19 Electronic Communications Act. As the provision has been in force for a comparably long time, the Government could argue that the data retention obligation is another development within this framework and therefore does not intervene with any potential constitutional rights.

56. To what extent and under which conditions does national law allow to draw on private actors for the purpose of law enforcement or any of the other purposes of data retention (as far as provided for by the national law transposing the Directive, cf. question 11)?

In a few very specific cases private actors are being obliged to take certain measures to facilitate law enforcement; one example being the information duty of banks with regards to money laundering. This is, however, not a general rule.

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

The constitution as such does not provide any arguments in this regard. The Swedish Government compared the obligation to adapt (see Q55) and the costs arising from this duty with other organisations' obligations to contribute to the interests of society in general (see e.g. Governmental Report SOU 2007:76 p 263). Examples for this include employer's responsibility to manage her employee's taxes and social security payments, or banks liability with regards to money laundering.

As the Government suggests that crime-fighting authorities share the costs with the providers, it will be difficult to argue that non-compensation for the additional costs would be unconstitutional, though providers with carry the main share of the costs for upgrading their systems. Authorities will reimburse the occurred costs for the release of data, not the retention of data.

III. Dimension 3 (State – State)

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

The European Convention for the Protection of Human Rights and Fundamental Freedoms was incorporated into Swedish law in 1994 and is guaranteed constitutional character in the Swedish Instrument of Government through its Chapter 2 Article 23. ("No act of law or other provision may be adopted which contravenes Sweden's undertakings under the European Convention for the Protection of Human Rights and Fundamental Freedoms.")

In general, international treaties have to be incorporated into Swedish law in order to be applicable in Sweden. An agreement can be transposed either by adapting it as a Swedish constitutional text, or by means of a separate legal act that stipulates the application of the agreement in Sweden. International treaties as such do not have a higher or lower status as Swedish legislation; it depends on their transposition into Swedish law.

59. Are there any situations/configurations that might concede to Directives a particular status within the hierarchy of norms of your country's legal system and/or grant them immediate effect? In general, what steps have to be followed in order to transpose a Directive into national law in your country?

The direct effect of Directives can be considered in accordance with EU law and the applicable case law by the European Court of Justice. There are no specific rules on direct effect in Sweden. As in all other Member States of the EU, EU law is a primary legal source in Sweden.

In general, transposition of Directives follows the same procedure as any other legislative process in Sweden. The Directives are traditionally discussed in a governmental report, which includes a draft for a bill and which is sent for public consultation. Then the Government compiles a legislative proposal, which is being presented to the parliament for voting.

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?

Chapter 10 Article 5 Swedish Instrument of Government specifically stipulates that the parliament may transfer decision making powers to the European Union to the

extent this does not "affect the principles of the form of government". These principles also include protection of fundamental rights. This provision in the Swedish constitutional law is the only explicit limitation for exercising EU competence.

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

The Governmental Official Report and the intended legislative bill are being discussed by the Ministry of Justice and the Ministry of Enterprise, Energy and Communications. It is, however, not clear at this point, to what extent any powers might be divided among various authorities.

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

No, not specifically.

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?

It is interesting to note, that several Swedish communication service providers have stopped retaining data due to the transposition of the Enforcement Directive and the newly stipulated right for e.g. copyright holders to be able to access subscription information for certain IP numbers through a court order. This shows the variety of public opinions on the topic and the difficulties to balance all different rights concerned as well as the possible consequences of data retention.

As the Governmental Official Report emphasised, statistical data is necessary to prove the importance of law enforcement agencies being able to access communications data. Information about communications has been used for law enforcement and crime solving measures already before the enactment of the data retention. In this regard it is important to ensure transparency and openness of surveillance measures by the police.

As the Swedish debate shows, the main issue seems to be access to traffic data by private entities, though a court order is necessary, not the general obligation to retain communications data.

From a legal point of view, the transposition of the Directive is only a matter of time, though it seems that a legislative bill leans towards meeting the minimum

requirements of the Directive as opposed to going further regarding the types of data retained.

From a political point of view, the recent parliamentary elections, a focus on general surveillance by the Swedish signal intelligence agency, and the Pirate Bay trials have taken a lot of attention from data retention issues the last two years and directed the discussions towards copyright and privacy, and less on law enforcement and privacy.

In my opinion, transposition of the Directive might bring clearance to the extent of data to be stored and kept by electronic communication service providers and provide answers to what extent existing data can be used by law enforcement agencies. In this regards, transposing the Directive as it is, while considering any amendments to the Directive on a European level, should be the way forward, in order to ensure a general level of harmonisation in the European Union.

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

Sweden

Christine Kirchberger

Part 2: Overarching issues and country-specific questions

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

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

The Swedish constitution allows for the right to be anonymous in various specific circumstances, e.g. regarding access to public information and providing the media with information. The latter stipulates that anyone supplying the media (press, TV, radio) with information has the right to be anonymous as the source. (Chapter 3 Article 1 The Freedom of the Press Act (*Tryckfrihetsförordning (1949:105)*).

Though both the Freedom of the Press Act and The Fundamental Law on Freedom of Expression (*Yttrandefrihetsgrundlag (1991:1469)*) contain chapters on "the right to anonymity" (Chapter 3 and Chapter 2, respectively) these mainly concern publishers of media and their sources (See http://www.riksdagen.se/templates/R_PageExtended____6333.aspx and http://www.riksdagen.se/templates/R_PageExtended____6346.aspx).

In addition, Chapter 2 Article 1 The Instrument of Government (*Regeringsformen (1974:152)*) grants freedom of expression and freedom of information. Chapter 2 Article 6 stipulates the protection against "eavesdropping and the recording of telephone conversations or other confidential communications" and "against significant invasions" of someone's privacy.

While all these provisions are important for the confidentiality of communications and their senders, they do not equate to a general right to communicate *anonymously*.

2. Please illustrate in detail any amendments to the current draft legislation on data retention that are 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?

The Swedish Parliament decided on 16 March 2011 to defer the vote on the proposed Government Bill (Prop. 2010/11:46) and a decision is not to be expected before May 2012. Despite a judgement by the European Court of Justice in February 2010 (C□185/09), the Directive has still not been transposed into Swedish law. Therefore, the European Commission has initiated further investigations into the failure of implementation by Sweden. See press release http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/409&format=HTML&aged=0&language=EN&guiLanguage=en

There has not been any further public discussion of the issues related to the transposition of the Directive.

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?**

   Besides the duty for communication providers (anpassningsskyldigheten) to manage their operations in a way that allows decisions on secret wiretapping and surveillance (Chapter 6 Section 19 Electronic Communications Act.), there are specific obligations for certain private actors. The Police Act only stipulates, in Section 3, that other public authorities should support the police in their work.

   Examples of obligations for private actors are regulated in various statutes and spread around Swedish legislation. They vary in content, but mostly concern providing the police with certain information. To name but a few:

   - Banks are obliged to reveal information to the crime fighting bodies with regards to money laundering (Money Laundering and Terrorist Financing (Prevention) Act - *Lag (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism*).

   - Auditors for Limited Companies are obliged to take necessary steps if they suspect certain crimes have been committed by the Chief Executive Officer or Board Members (Companies Act - *Aktiebolagslag (2005:551))*

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?

Chapter 36 Section 6 of the Code of Judicial Procedure stipulates that a "witness may decline to testify" about a circumstance that should reveal that she/he, or a person related to her/him has committed a criminal or dishonourable act. This is, however, not comparable to a right to refuse to testify as is stipulated in Chapter 36 Section 3 and which applies to spouses and relatives.

Section 6 is only relevant for testimonies in front of the court. In other words, a person can only refuse to testify after being asked a question during court proceedings. If a person exercises this right, the court has the possibility to use previously given statements made by the person before a court, a prosecutor or a police authority (Chapter 36 Section 16).

As these provisions clearly give the possibility to use earlier evidence and even direct statements by the accused, it does not seem likely that data retained from earlier communication would not be possible to be used as evidence in court.

Concerning lawyer-client privilege, the Governmental Official Report preceding the Governmental Bill (*SOU 2007:76 - Lagring av trafikuppgifter för brottsbekämpning*) mentioned that it would be technically unfeasible and interfere with the principle of privacy if electronic communications providers would not be allowed to store data covered by the lawyer-client privilege stipulated in Chapter 36 Section 5. The privilege is, however, not too strong, as secret surveillance is possible concerning people covered by Section 5 (See Chapter 27 Section 20 Code of Judicial Procedure). Furthermore, the Electronic Communications Act (*Lagen (2003:389) om elektronisk kommunikation*) does not contain any specific provision not allowing the release of electronic communications data to the entitle bodies. In other words, it is not explicitly forbidden to retain or release communications data. The principle of proportionality applies, however, to all kinds of coercive measures and might in practice limit the possibility for crime fighting authorities to access communications data between a client and her/his representative (See Chapter 27 Section 1 Code of Judicial Procedure and Section 8 Police Act (*Polislag (1984:387)*). In short, the principle states that coercive measures only may be imposed if the reasons for the measure outweigh the intrusion or other detriment to the suspect or to another adverse interest.

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?**

As the Directive has not been transposed yet, there is no detailed information on this question. As the official authorities in general have to follow extensive data protection legislation, however, one could assume that the general applicable laws will also cover circumstances of retained data being held by public bodies. Chapter 18 Section 1 Public Access to Information and Secrecy Act (*Offentlighets- och sekretesslag (2009:400))* establishes secrecy for information related to the police

investigation, and the Swedish Police Data Act (*Polisdatalag (1998:622)*) regulates personal data processing by the police and basically stipulates the requirements the police have to fulfil when processing any types of personal data. The Police Data Act contains, inter alia, provisions on what types of personal information can be stored, which databases the crime fighting authorities can run, as well as rules on deletion of data.

The Government Bill (Prop. 2010/11:46) proposing the transposition of the Directive mainly deals with security and organisational measures to be performed by the communication providers, not the entitled bodies. This could lead to the conclusion that the general obligations that crime-fighting authorities fall under, such as the Police Data Act, apply for the retained data as well as for the general data held by the bodies.

Interesting to note is that the rather strong protection for whistle blowers (*meddelarfrihet*) (Chapter 13 Section 1 Public Access to Information and Secrecy Act) does not apply in cases where information concerning police investigations (Chapter 18 Section 1 Public Access to Information and Secrecy Act) is being revealed (See Chapter 44 Section 4 Public Access to Information and Secrecy Act). In other words, a person sharing data on secret wiretapping (*hemlig teleavlyssning*) or surveillance (*hemlig teleövervakning*) can be fired, face disciplinary actions and also pay a fine or be imprisoned up to 1 year (Chapter 14 Section 1 same Act).

The Swedish Government is currently revising the provisions on secret wiretapping (*hemlig teleavlyssning*), surveillance (*hemlig teleövervakning*) and access to data according to the Electronic Communications Act. Three Governmental Official Reports have been published in the last years, and were followed by an Opinion of the Council on Legislation (*Lagrådet*) in December 2010 (*De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation*, http://www.regeringen.se/sb/d/12658/a/158026). A Governmental Bill (*De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation, Prop. 2011/12:55*) was published in February 2012 in this regard (http://www.regeringen.se/sb/d/15227/a/186055).

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.**

As the Directive has not been transposed yet, the only data available concerns legislation not stipulating any obligation to retain data. The Swedish police and Prosecution Authority publish an annual report on the use of secret wiretapping. The latest one concerns 2009 (in Swedish at http://www.riksdagen.se/webbnav/index.aspx?nid=37&rm=2010/11&bet=66&typ=prop) but, unfortunately, does not list the requests based on the Electronic Communications Act (*Lagen (2003:389) om elektronisk kommunikation*).

In a governmental report from 2009 (*SOU 2009:1 En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen*) the police estimated that it had

requested data according to Chapter 6 Section 22 Electronic Communications Act in 9500 instances in the year 2007. The report explicitly stated that no detailed statistics were available at the moment.

The recent Government Bill (Prop. 2010/11:46) suggests statistics to be collected once the Directive is transposed.

B. Country-specific questions

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

While Chapter 2 Article 6 Instrument of Government (*Regeringsformen (1974:152)*) protects people against invasions of privacy, Chapter 2 Article 20 allows for limitation of these rights if stipulated by law. In this sense the data retention regime is in line with the Swedish constitution to the extent it regulates any obligations in legislation and not ordinances approved by the Government or another public authority.

Chapter 2 Article 21 Instrument of Government, however, requires these limitations to be adequately related to the purpose they attempt to regulate. The main question here is if general retention of data concerning people that are not suspects for any crime is beyond the purpose of crime fighting. The Government Bill clearly states that the purpose is adequate for data retention. In my opinion, it depends if there are any other, less intrusive, measures that can serve the purpose of detection and solving of crimes. Any investigations in this regard have not taken place, neither on an EU level nor on a Swedish level. The simple fact that electronic communication providers today have access to large amounts of data has lead to the believe that use of this data can help crime fighting bodies in their work. While this might be the case, it is not clear if there are any other, less intrusive, ways to find perpetrators and fight crime.

Due to the lack of appropriate alternative measures and the focus on data collection and data mining when solving crimes, it is difficult, however, to argue that data retention goes further than necessary with regards to its purpose. In other words, though the regime is within its constitutional limits, this might not always be the case in the future. Especially statistics on how much data retention can increase the amount of crimes solved will help in this regard.

In addition to privacy aspects, the question of reach of potential duties for private entities can be discussed. The constitution does not explicitly determine this question, but an in-fact-outsourcing of police work might affect issues of democracy and fair trial. Arguments of this kind have not been discussed which makes it difficult to assess their impact.

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

   The 2010 Governmental Bill explicitly exempts the content of communications from the data retention obligation. According to the wording of Chapter 2 Article 6 of the Instrument of Government everyone shall be protected against "against examination of mail or other confidential correspondence, and against eavesdropping and the recording of telephone conversations or other confidential communications". As for other fundamental rights, limitations can be stipulated in law (Chapter 2 Article 20). Traditionally, Article 6 protects the content of communications and not meta-data on a communication.

   Though not on a constitutional level, Chapter 6 Section 20 Electronic Communications Act stipulates a principle of confidentiality of communications, which includes subscription, traffic and location data as well as the content of an electronic message.

9. **Please describe the 2010 legislative proposals on the basis of questions 7 to 35 of the first questionnaire (please reply question by question) and explain how they differ from the 2007 governmental report as described in your answers to the first questionnaire.**

   The answers in the first questionnaire represented the views of the 2010 legislative proposal, though the 2007 report was mentioned on several occasions. The main differences concern the period of retention and the regulation of the specific types of data in legislation as opposed to ordinances and other regulations. Two aspects in the Swedish proposal that go further than the Directive regard data on unsuccessful call attempts to be stored and localisation data at the end of a communication, not only the start of a communication as the Directive stipulates.

   The 2007 Governmental Official Report suggested that the details for the data retention should be dealt with in an ordinance while the 2010 Governmental Bill contains the type of data that should be retained together with the purpose of retention, and regulates them in the Electronic Communications Act.

   The technical areas to be covered by data retention are, according both to the 2007 Report and the 2010 Bill:

   - Telephony (electronic communication service that allows the possibility to call or receive calls via one or several numbers within a national or international numbering plan)

   - Messaging (exchange or transfer of electronic messages, which are not conversations, or information, which is transmitted as part of a radio or TV programme. This definition may be slightly different to the one chosen in the Directive.

- Internet access (the possibility to transmit IP packages which give the user access to the Internet)

- Type of connection (the capacity which is offered to get Internet access; this area is not specifically mentioned in the Directive)

While the 2007 Official Report suggested one year as the period of retention, the Government Bill proposes 6 months. Data that has not been requested by the crime fighting authorities within 6 months is to be destroyed.

Both the Government Bill, as well as the Governmental Official Report from 2007, underline the importance of safeguarding that retained data is not used or spread unauthorised.

Both the 2007 report and the 2010 bill propose that all electronic communication providers who have to register their services, according to the Electronic Communications Act with the Swedish supervisory authority, Swedish Post and Telecom Agency (PTS), fall under the obligation to retain data. PTS can in certain cases decide on exemptions from the data retention obligation. This possibility is to be granted very restrictively, however, and only be granted after consultation with representatives from the crime fighting authorities.

As mentioned earlier, the 2010 legislative proposal deals only with the retention obligation for electronic communications providers and not with the details of release of this information to crime fighting authorities. These questions are being dealt with in the current revision of the legislation, with the latest publication being the Opinion of the Council on Legislation (*Lagrådet*) in December 2010 (*De brottsbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation*, http://www.regeringen.se/sb/d/12658/a/158026).

Depending on the crime fighting authority holding the data, different specific data protection acts apply. Besides the Public Access to Information and Secrecy Act stipulating secrecy for information being used in the police investigation preparing the court proceedings, the Police Data Act regulates data protection obligations for data held by the police. The Act was recently changed and the new Act (*Polisdatalag (2010:361)*) is entering into force in March 2012. The new Act will enable easier information sharing between Swedish crime fighting authorities and also facilitate international cooperation between authorities. Already the current applicable act (1998:622) allows the Swedish police to share information with other national authorities and hand over information to a foreign authority if the release is based on an international agreement that Sweden is a member of. In addition, Section 7 allows for cooperation with countries within Interpol.

10. How does the government intend to deal with possible sanctions (in particular those resulting from EU infringement proceedings before the ECJ) as a consequence of the non-transposition of the Directive?

The Government has not released any information concerning this question.

11. **Is the constitutionally fixed limit to a conferral of national sovereignties to the EU (see your answer to question 60 of the first questionnaire) in any way binding for representatives of your country in EU organs and institutions (e.g. the Council of Ministers, the European Council) when exercising their functions in the adoption and execution of an EU legislative act?**

    Swedish ministers represent Sweden and must pursue the line that the government has received support for in the Committee on EU Affairs. The government discusses proposals with the Parliament in advance, as Parliamentary support is required. Swedish representatives are therefore bound when exercising their functions.

    If a Parliamentary committee considers a legislative proposal from an EU institution to go against the subsidiarity principle, the committee submits an opinion to the Parliament that, if approved, can be sent on to the European Parliament, Council of Ministers and EU Commission.

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

    When describing the different technical solutions of data retention, both the 2010 Governmental Bill and the earlier Governmental Official Report 2007:76 mentioned the possibility that certain data might be retained by several providers in certain cases, but did not consider this a major legal challenge. The argumentation concerned the question if a centrally administered storage would be preferred to each provider storing the data created in its systems.

    Regards for privacy seemed in favour of a locally distributed storage where each network operator or service provider is responsible for retaining the data created in its system. Though this might involve data being stored at several locations, the Government considered it to be less intrusive than a central storage where all available data could be connected and mined.

    In order to allow smaller providers to avoid too high costs the 2010 proposal suggests the possibility to outsource the storage of the communications data. This does, however, not release the provider from its data protection obligations, but only offer an option for the technical storage to be done at a third party.

13. **If (partial or full) cost reimbursement is regulated in the 2010 draft: please describe the applicable reimbursement rules in detail (as far as this is possible at the current state of play). In which form and to which extent (completely, certain percentage of the full costs, lump sum, mere depreciation of book-entry items on tax return) are the costs reimbursed? How and by whom (government authority, provider) are the amounts to be reimbursed calculated? How are the specific data retention costs delimited against the costs for the general storage equipment and the general data storage process?**

The 2010 legislative proposal suggests that the electronic communication providers carry the costs for storage, security and adaptation of the systems, while the crime fighting authorities reimburse the costs of the providers for releasing the information in each specific case. According to the proposal this is the most suitable solution as the incurred costs are split between the providers and the authorities. Providers are, in this scenario, inclined to keep the costs of storage down, while police authorities will not ask for data unless it is absolutely necessary, as the total costs would increase otherwise.

The 2010 Governmental Bill does not mention any specific amounts for reimbursement yet. The decision of the suitable amounts of reimbursement will be up to the Government or the authority appointed by it. It seems likely that the supervisory authority will publish set fees for different types of release of information by the providers, which will lower the administrative burden to calculate the incurred costs in each case. According to the proposal both crime fighting authorities as well as communication providers estimate the costs between 1500 and 2000 Swedish kronor (ca 150 – 200 €) per instance.

The proposal estimated the total costs of storage etc. to approximately 200 million Swedish kronor (ca 20 Mio €) and the costs for reimbursement by the authorities up to 20 million Swedish kronor (ca 2 Mio €) per year. Though the numbers have been difficult to predict, and vary depending on who is estimating the amounts, the Government and several other authorities and organisations seemed to acknowledge them when responding to the original Governmental Report from 2007.