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

Denmark

Associate professor Charlotte Bagger Tranberg, ph.d., Aalborg University

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

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

I. Legal provisions

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

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

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

The provisions of the Directive have already been transposed into Danish law. Before the passing of The Data Retention Directive rules existed on data retention in Danish law. The rules were inserted in the Danish Administration on Justice Act immediately after the terror attack on New York on 11th of September 2001. But already before that there had been considerations about data retention in respect of solving crimes on child pornography. The bill that introduced data retention rules in to Danish Law was adopted in 2002, but the provision on data retention did not come into force before the 15th of September 2007. The passing of the data retention

directive entailed the issuing of a Ministerial Order on data retention, which regulated the provider's obligation to retain data in detail.

The Ministry of Justice underlined that the bill from 2002 did not entail that the internet service providers must map the consumers activities on the internet. The providers were not being imposed to register every homepage, chat rooms etc. visited by the consumers. The intention with the bill was to follow the electronic traces regarding criminal activities on the internet back to the perpetrators. The Ministry of Justice also found that there should not be made demands on a general logging of the content of the information, but only information corresponding to telephone information – sender, recipient and indication of time of the communication. The solution did not give the police access to the logged information. The question must be dealt with according to provisions in the Danish Administration on Justice Act on interception on communication.

- **If transposition has not at all, or only in parts, 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)?**

   ---

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?**

   ---

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.**

- ***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.**

   Unfortunately not.

   Administration of Justice Act:

   https://www.retsinformation.dk/forms/r0710.aspx?id=133272#K71_2

Danish Ministerial Order on Data Retention:

https://www.retsinformation.dk/Forms/R0710.aspx?id=2445

Danish Ministerial Order on practical Support of providers of electronic communications networks or communications services to the police regarding interception of communication (24-hours point of contact):

https://www.retsinformation.dk/Forms/R0710.aspx?id=2491

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 in the Administration of Justice Act have been into force since 15th of September 2007, but as mentioned earlier on the rules was adopted June 8th 2002.

   There are no transition periods 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**

      - Administration on Justice Act, section 786, (4 and 5)
      - Danish Ministerial Order on data retention
      - Danish Ministerial Order on practical support of providers of electronic communications networks or communications services to the police regarding interception of communication (24-hours point of contact)
      - There are two ministerial orders: One on data retention and one on 24-hours point of contact

   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.**

      In the first version of the bill on data retention from 2002 it was the opinion that the regulation should only be a Ministerial Order because of practical and legal technical reasons. However, the Ministry of Justice changed position. Therefore the obligation to data retention now appears from the Danish Administration on

Justice Act. The new provision on data retention in the Administration on Justice Act was inserted to ensure that the obligation to register and store traffic data, including the retention period, must be a provision in an act.

The technical implementation of the obligation to the data retention will appear from a ministerial order. The character and a level of detail of the specific retention provisions imply that it will not be appropriate to provide the provisions by an act. Furthermore it will be quite complicated to introduce a bill, when there may be a need for justification of the provisions that will have technical character to a certain extent. It will be more flexible that justifications can be made by changing a ministerial order.

This is the Danish Ministerial Order on data retention

The legal basis for data retention is in the Administration of Justice Act section 786 (4 and 5).

The Danish Ministerial Order on data retention is issued with legal basis in the Administration of Justice Act section 786 (4)

The Danish Ministerial Order on practical Support of providers of electronic communications networks or communications services to the police regarding interception of communication (24-hours point of contact) is issued with legal basis in the Administration of Justice Act section 786 (5)

The Danish Ministerial Order on data retention contains the rules on data retention. The Danish Ministerial order on 24-hour point of contact contains an obligation for providers of electronic communications network or communications services to end users to establish a 24-hour point of contact that at any time can assist the police regarding interception of communication. Small providers can apply the National Commission of the Danish Police regarding permission to establish a on-call service, where the police can make an application to certain employees or representatives for the provider, who can ensure the appropriate in connection with interception of communication.

The Danish Ministerial Order on 24-hour point of contact does not apply for housing cooperatives, house-owners' associations, cable service providers and similar organization or associations within providing electronic communications networks or services to fewer than 100 units.

Because the provisions on obligatory retention of data on telecommunication traffic for the purpose of investigation and criminal prosecution were innovative in relation to the former state of the law, the Ministry of Justice suggested that the solution was evaluated some years after the implementation. Cf. question 49 on the debate on the revision of the provisions.

8. **Are the terms defined in art. 2 para. 2 of the Directive also defined within the national law transposing the Directive? If so: To what extent do the definitions**

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

The terms defined in art. 2 para. 2 of the Data Retention Directive are not defined within the national law transposing the Directive – neither in the Danish Administration of Justice Act nor in the Danish Ministerial Order on data retention.

However, the guidance to the Danish Ministerial Order on data retention underlines on several points that the terminology used in the Order correspond to the terminology in the Directive.

The definitions mentioned in Directive 95/46/EC are all defined in the same way in the Danish Data Protection Directive.[1]

Some of the definitions in Directives 2002/21/EC and 2002/58/EC have been legally defined in the national legislation.

The Act on Competitive Conditions and Consumer Interests in the Telecommunications Market[2] defines art. 2(a), 2(c), 2(f), 2(n) and 2(p) in the Directive 2002/21/EC. The wordings of the definitions in the Danish act are not exactly the same as in Directive 2002/21/EC.

The wording is not the same but the meanings of the definitions are the same as in 2002/21/EF

The Ministerial Order on the Provision of Electronic Communications Networks and Services[3] defines art. 2(a), 2(b), 2(c) and 2(g) in Directive 2002/58/EC. The wordings of the definitions are equivalent to those in Directive 2002/58/EC.

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?

---

1 Act No. 429 of 31 May 2000, Section 3. http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/read-the-act-on-processing-of-personal-data/the-act-on-processing-of-personal-data/

2 Consolidated Act No. 780 of 28 June 2007, Sections 3(1), 3(2), 7a, 4, 7b

3 Ministerial Order No. 714 af 26 June 2008, Sections 2(3)-2(6). http://en.itst.dk/telecom-internet-regulation/filarkiv-obligations-for-suppliers/executive-order-on-the-provision-of-electronic-communications-networks-and-services

A provider of electronic communications network or communications services to end users must retain the following data concerning fixed network telephony and mobile telephony and SMS-, EMS- and MMS-communication:

1) The calling telephone number and the name and address of the subscriber or registered user.

2) The called telephone number and the name and address of the subscriber or registered user.

3) Change in the called telephone number (call redirection) and the name and address of the subscriber or registered user.

4) Receipts for receiving of messages (SMS, EMS, MMS).

5) Identity on the used communication equipment (IMSI and IMEI).

6) That or those cells a mobile phone is connected to at the beginning and the end of the communication and the precise geographic and physic position of the matching telephone poles.

7) The time of the beginning and the end of the communication.

8) The time for the first activation on pre-paid anonymous services.[4]

A provider of electronic communications network or communications services to end users must retain the following data concerning the initial and final packet of an internet session (or the use of internet telephony):

1) The calling Internet Protocol address.

2) The called Internet Protocol address.

3) The Transport Protocol.

4) The calling port number.

5) The called port number.

6) The time of the start and end of the communication[5].

The obligation to retain data concerning the initial and final packet of an internet session does not apply to providers of electronic communications network or communications services to end users if the retaining is not technical possible in the system of the provider. If retaining is not technically possible the provider must retain the data for every 500rd packet that is included in the end users internet

---

4 Danish Ministerial Order on data retention, section 4.

5 Danish Ministerial Order on data retention, section 5, para. 1.

communication. The exact time for retaining the data about the packet must also be retained.[6]

The retaining of the data mentioned above (1-6) must take place at the transfer between the providers own network and any other networks.[7]

A provider of electronic communications network or communications services to end users must also retain the following data concerning a user's access to the internet (or the use of internet telephony):

1) The user ID(s) allocated.

2) The user ID and telephone number allocated to any communication entering the public telephone network.

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

4) The time of the start and end of the communication.[8]

Providers of electronic communications network or communications services to end users, who provide wireless internet access, must also retain data on the precise geographic and physic position of the used local network and the identity on the equipment for communication.[9]

The retaining of the data mentioned above (1-4) must take place at the transfer between the providers own network and any other networks.[10]

Providers of electronic communications network or communications services to end users must also retain data on the calling and the called e-mail address on their own e-mail services.[11]

The rules do include additional retention obligations with regard to traffic data which go beyond the obligations mentioned in the Directive. The additional retention obligations relates to changes in the called telephone number (call redirection) and the name and address of the subscriber or registered user and receipts for receiving of messages (SMS, EMS, MMS). In Denmark data on internet sessions must also be retained.

---

6 Danish Ministerial Order on data retention, section 5, para. 4.

7 Danish Ministerial Order on data retention, section 5, para. 5.

8 Danish Ministerial Order on data retention, section 5, para. 2.

9 Danish Ministerial Order on data retention, section 5, para. 3.

10 Danish Ministerial Order on data retention, section 5, para. 5.

11 Danish Ministerial Order on data retention, section 6, para. 1.

Data on unsuccessful call attempts have to be retained.[12]

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.

According to the Ministerial Order on the Provision of Electronic Communication Networks or Services a provider of electronic communications networks or services is permitted to process and store traffic data for the purposes of subscriber billing and interconnection payments.[13]

A provider of public electronic communications networks or services is permitted to process traffic data regarding subscribers or users for the purpose of marketing electronic communications services or for the provision of value added services if the subscriber or user has consented thereto.[14]

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

For the investigation and prosecution of criminal offences.

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

The Administration of Justice Act contains a number of provisions, which intercept the police in intercepting communication between the suspect and persons with a special relation to the suspect. Priests, doctors and lawyers do not have to testify about secret information gathered in relation to their jobs.

In fact, these provisions entail a protection of the communication between a suspect and the persons mentioned just above. The provisions originate in the relationship of confidence between a suspect and this group of persons.

According to the main provision in the Administration on Justice Act it is not possible to intercept communication between these persons but the provision does

---

12 cf. The guidance to the Danish Ministerial Order on data retention, section 2.1.1.

13 Danish Ministerial Order on the Provision of Electronic Communication Networks or Services, section 28(2).

14 Danish Ministerial Order on the Provision of Electronic Communication Networks or Services, section 28(3).

not include telecommunication records. The reasons for this exemption are practical considerations and the fact that the content in the communication is not being disclosed. This means that the special relationship of confidence is not being disputed.

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.

Retained data must be kept available for 1 year.[15] There is no distinction to data categories.

The Ministry of Justice was aware of the difficulties balancing combating crimes on one hand and the privacy and the expenses on the providers on the other hand. Particularly the privacy considerations dictate the least possible retaining and that the retained data are being retained for the shortest period as possible, because a long retaining period means higher risk of the data falling into the wrong hands.

The Ministry of Justice found that a 12 month retention period covered the need of the police to access data in a specific case. The Ministry of Justice found it doubtful that a 6 month retaining period covered the police´s need for access to data. It is the opinion of the Ministry of Justice that even terror attacks of lesser extent than the attacks on New York and Washington on 11th of September 2001 normally take a long period to plan.

The length of the retention period has been discussed several times in Denmark.

The first time was in relation to the duty to inform the EU-commission about the use of data retention in Denmark. In this case it was the question if the Danish retention period on 12 months was an absolute storage period for the data, or if the providers could store the data for a longer period. The Ministerial Order on Data Retention does not contain provisions on the provider's obligation to delete data at the expiry of the Danish retention period. According to the Ministerial Order on the Provision of Electronic Communication Networks or Services, section 28(2). Providers of public electronic communications network or communications services must ensure, that traffic data on subscribers or users are deleted or anonymised when they are no longer necessary for the communication. However, it was permitted that providers store data for certain purposes, including billing or obligations that originate from the Ministerial Order on Data Retention.

The second time was in relation to the suggestion from the Ministry of Justice that intended to remove the provision on revision the data retention provision in the Administration on Justice Act, cf. question 49.

---

15 Danish Administration on Justice Act, section 786, para. 4 and Danish Ministry Order on Dataretention, section 9.

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)?

According to the Administration on Justice Act, section 780 (3 and 4) the police and the Danish Security Intelligence Service can intercept the communication by gathering information relation to telephones or other similar instruments for communication that are connected to a certain phone or another similar instrument for communication - even though the owner of this have not given permission to it (telecommunication records) and information on, which telephones or other similar instruments for communication within a disclosed area, there are in connection with other telephones or similar instruments for communication (extended telecommunication records)

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

The retained data may only be used for enforcement (Investigation and prosecution) of a serious crime, cf. question 14 and 16, if the provisions on interception of communication are respected.

The access to retained traffic and location data is considered to be a case of communication interception.

Extended communications records are outlined in question 14.

The national law does not grant any rights to individuals to access the data retained directly, cf. the view of the Danish trade union for IT-professionals PROSA in question 49.

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)?

The specific requirements can be found in the Administration on Justice Act on interception of communication.

The specific conditions for interception of communication are *firstly,* that there must be certain grounds for assuming that messages to or from a suspect are covered by the communication in question. The collection of extended telecommunications records may only be carried out where the suspicion concerns an offence that has caused or may cause danger to human welfare or community property of substantial value. *Secondly,* the interception of communications is assumed to be of decisive importance to the investigation. The *third* and last condition is a requirement as to

the nature of the crime, particularly that the investigation concerns a offence with a maximum penalty exceeding six years or contravention of Parts 12 and 13 in the Danish Criminal Code[16].[17]

The rule on interception of communication also implies a rule of proportionality. According to this provision, the interference may not take place if, in view of the purpose of the interference, the importance of the case and the outrage and inconvenience that the measure is assumed to cause will constitute a disproportionate intrusion.[18]

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?

Any interception of communications must take place on the basis of a court order, and the court order must indicate, for example, the telephone number that is the target of interception. In practice it has been accepted that the telephone to be tapped may be identified by other numeric codes than the telephone number, such as the IMEI or IMSI number of a mobile phone.[19]

If the purpose would be defeated by awaiting prior permission from the court, the police may decide to carry through a measure of interference. However, the matter must be put before the court as soon as possible and no later than 24 hours after implementation of the measures, whereupon the court will decide whether the interference can be approved and may be continued, if required.[20]

The wording 'as soon as possible' must be taken literal. In one specific case the court point out that the permission was delivered to the court after 18 hours (UfR1980.285Oe). There is no material answering the question when the 24-hours limit starts.

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

The Administration on Justice Act contains obligations to appoint a lawyer for the person that the interception concerns.[21] The lawyer must protect the aggrieved party

---

16 Offences against the independence and security of the state and offences against the Constitution and the supreme authorities, terrorism etc.

17 Danish Administration on Justice Act, Section 781(1)(1-3).

18 Danish Administration on Justice Act, Section 782(1).

19 Danish Administration on Justice Act, Section 783(1).

20 Danish Administration on Justice Act, Section 783(3).

21 Danish Administration on Justice Act, Section 784(1)

in the court. The lawyer can not pass any received information to anyone or make contact with the aggrieved party without consent of the police.[22]

The lawyer must protect the suspects and others peoples interests and ensure a contradictory discussion of the interception.

After ending an interception of communication there must be given notification to the aggrieved party. In case of interception in telecommunication records notification must be given to the holder of the telephone.[23]

It is only possible to access data if the rules in the Danish Administration of Justice Act are respected.

In case of interception in *extended* telecommunication records there must *not* be given notification to the holders of the concerned telephones.[24] Interception of extended telecommunication records normally include so high number of persons that notification is not possible in practice.

The notification can also be omitted if the notification will be damaging to the police investigation in this case, in other pending cases about interception of communication or for the protection of the investigation methods of the police. The court must decide if the notification is to be omitted or postponed.[25]

The provision is normally been used in cases about organized and systematic crime and in investigation with in groups of organized crime e.g. biker gangs.

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

The aggrieved party does not have the right to be informed about the data accessed, only that there has been an inception of communication. According to the Danish Act on Processing of Personal Data the controllers responsibility to give information to the data subject does not apply to processing of data which is performed on behalf of the courts in the area of criminal law and to processing of data which is performed on behalf of the police and the prosecution in the area of criminal law.[26]

---

22 Danish Administration on Justice Act, section 788.

23 Danish Administration on Justice Act, section 788(1).

24 Danish Administration on Justice Act, section 788(5).

25 Danish Administration on Justice Act, section 788(4).

26 Danish Act on Processing of Personal Data, section 2(4).

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

The role of the lawyer appointed to the aggrieved party is also to make sure that possible questions in relation to the interception of communication are appealed to a higher court.

The aggrieved party does not dispose of any recourse neither before nor after the notification.

The appointed lawyer must protect the aggrieved party. As far as I have been able to find out there are no possible recourses for the aggrieved party afterwards. The appointed lawyer must do a eventually recourse.

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.

The rule on security in relation to processing of personal data in the Danish Act on Processing of Personal Data does also include retained data.[27]

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

The police must destroy material provided by interception of communication if there are not pressed charges against the person in question for the infringement of the law on grounds of the interception of communication or if legal action is being dropped later on.[28]

Material procured by interception of communication that does not have importance to the investigation must be destroyed.[29]

The police must also comply with the principle on time limitation in the Danish Act on Processing of Personal Data.[30] According to this provision the data collected may not be kept in a form which makes it possible to identify the data subject for a longer period than necessary for the purposes for which the data are processed.

---

27 Danish Act on Processing of Personal Data, section 41.

28 Danish Administration on Justice Act, section 791(1).

29 Danish Administration on Justice Act, section 791(4).

30 Danish Act on Processing of Personal Data, section 5(5).

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.

'Providers of electronic communications networks or services to end users' can be defined as parties that put electronic communications network or communications services at several users disposal on a commercial basis. The terms electronic communications network and electronic communication service are defined in accordance with the definitions in Directive 2002/21/EC art. 2(a) and 2(c). The term *'end user'* is defined in accordance with the definitions in Directive 2002/21/EC art. 2(n).

Every company that serve more than one end user on commercial basis are included in the definition. It is insignificant whether or not the provider has its own infrastructure, whether it is public available or closed networks, ad furthermore, the extent and the kind of the services are also insignificant. Companies with own network that only provide infrastructure to the company itself are not covered by the definition.

The Danish legislation on telecommunication does not provide an independent definition on the term *'commercial basis'*. It will be evaluated from time to time and from case to case. 'Commercial basis' means a person, a company or a public body that sell and market a product to make profit. It is insignificant if the product yields a profit or a deficit. The term commercial basis implies that libraries, educational institutions (e.g. universities) and other public bodies that – on a non-commercial basis – provide net and services for persons that are external parties, ex. students, borrowers, patients in hospitals and similar persons do not have to retain data. It is also the case for workplaces that put telephone and internet access at the disposal of employees on a non-commercial basis. These non-commercial providers are not part of the data retention obligation in the Danish Ministry Order on data retention.

On the other hand, hotels and camp-sites are assigned to retain data in accordance with the Danish Ministry Order on data retention both if they offer wired and wireless access to their guests.

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?

Housing cooperatives, house-owners' associations, cable service providers and similar organization or associations within providing electronic communications networks or services to fewer than 100 units.[31]

[31] Danish Ministerial Order on data retention, section 3.

Transport of radio and TV programs.[32]

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 police and the Danish Security Intelligence Service can intercept the communication by gathering information relation to telephones or other similar instruments for communication that are connected to a certain phone or another similar instrument for communication - even though the owner of this have not given permission to it (telecommunication records). According to the provision the police can retain data on telecommunication regarding certain telephone numbers, for instance information on phone calls to and from a suspect.[33]

Since 2001 there has been a provision in the Danish Administration on Justice Act, after which the police can intercept communication by gathering information on, which telephones or other similar instruments for communication within a disclosed area, there are in connection with other telephones or similar instruments for communication (extended telecommunication records). The provision gives the police an opportunity to get access to the so-called telephone pole information regarding investigation of offences that has caused or may cause danger to human welfare or community property of substantial value.[34]

The two provisions mentioned above provided the police with an access to telecommunication records that providers registered and stored for other purposes (especially for billing). The provisions did not require that the service providers retain certain telecommunication records. The police could get access to data already stored by the providers for other reasons.

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)?

According to the Act on Competitive Conditions and Consumer Interests in the Telecommunications Market the owners of telecommunication networks and the providers of telecommunication networks or telecommunication services must secure that data about other peoples use of the network, the service or the content of the information does not fall into the hands of unauthorized persons.[35]

---

32 Danish Ministerial Order on data retention, section 2.

33 Danish Administration on Justice Act, Section 780(1)(3).

34 Danish Administration on Justice Act, Section 780(1)(4).

35 Danish Act on Competitive Conditions and Consumer Interests in the Telecommunications Market, section 13(3).

The owners of telecommunication networks, the providers of telecommunication networks or telecommunication services, the employees and former employees in these companies must not unjustified pass or use data on others peoples use of the network, the service or the content of the information which they get access to in connection with the concerned supply of electronic communication networks or electronic communication services.[36]

The provisions in the criminal law on confidential information can also be used in respect of a person that is or has been employed at the owner of a telecommunication network or the provider of telecommunication networks or telecommunication services. The provisions can also be used regarding a person that is or has been employed with assignments conducted on an agreement with these owners or providers.[37]

According to the Ministerial Order on the Provision of Electronic Communications Networks and Services the providers of public electronic communications networks or communications services shall in preparation for network security implement appropriate technical and organizational security measures to protect the offered services. If necessary this must happen in corporation with the owner or the provider of the used public communication network.[38]

The providers of public electronic communication networks or -services must give the subscribers information about potential special risk on breach of network security. The providers must also give information on the possibility to prevent such breaches and the cost connected with this.

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)?

Non-official numbers mention 200 mio. DKK for the establishment and 50 mio. DKK every year for the running operations.

---

36 Danish Act on Competitive Conditions and Consumer Interests in the Telecommunications Market, section 13(1).

37 Danish Act on Competitive Conditions and Consumer Interests in the Telecommunications Market, section 13(2).

38 Danish Ministerial Order on the Provision of Electronic Communications Networks and Services, section 31(1).

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

The obligated parties do not receive reimbursement for their costs by the government.

According to the Administration on Justice Act the Minister of Justice can provide provisions on economic reimbursement to companies for direct costs related to the assistance to the police in intercepting communication.[39] It is provided that reimbursement only covers costs in relation to the interception. The authorisation is not exploited.

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

Danish Ministerial Order on practical support of providers of electronic communications network or communications services to the police regarding interception of communication (24-hours point of contact). See question 6b.

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 the Ministerial Order on Data Retention providers lacking abidance of the provisions on retention can entail punishment in the form of a fine. Companies can entail punishment after chapter 5 in the criminal code.[40]

The sanction is a criminal penalty. Violation of section 4, 5, 6 and 9 in the Danish Ministerial Order on data retention are being fined.

Criminal Code sec. 25-27, especially section 27. Criminal liability for legal persons require that there is committed a crime that can proven to be one or more persons affiliated to the company fault or proven to be the legal persons fault as such.

---

39 Danish Administration on Justice Act, section 786(8).

40 Danish Ministerial Order on Data Retention, section 10.

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?

Only the police can access the retained data.

The SIS must make a request to the court as a police authority in accordance with Administration of Justice Act section 783.

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?

There are not any regional entities vested with own authority that have been granted their own rights of access to the retained data.

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

None

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)?

Exchange of retained data with other EU Member States, EEA Member States and third countries takes place on legal basis of the provision in the Administration of Justice Act.

The requests must fulfil the 'normal' requirement for interception of communication according to the Administration of Justice Act.

I am not sure and it has not been possible for me to find any exact information, but I guess that all requests must fulfil the requirement for interception of communication in the Administration of Justice Act.

The police serve as a single point of contact for the transmission of all outgoing requests. All outgoing requests must be handled by the police.

Foreign states do not have direct access to the retained data. The foreign states have to send a request to the Danish police.

The Danish police send a request to the court. The court judges if the requirement for interception of communication in the Administration on Justice Act is for fulfilled.

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 Data Protection Authority is by law independent from the Ministry of Justice, but that may not be the actual case in practice.

The National IT and Telecom Agency is a part of the Ministry of Science, Technology and Innovation. Both comprehensive supervisory control in terms of both legality and technical advisability is applied

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

If so, please answer to the following questions:

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

n/a

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

n/a

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?

n/a

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?

The data are stored locally by the service providers, but it is possible that the retention can be done by another provider or a third party.[41]

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?

Data can only be stored outside Denmark in accordance with data protection legislation, an EU-country or a third country which ensures an adequate level of protection.

It is a question on establishment. If the controller is established in Denmark it must comply with the Danish Act on Processing of Personal Data.

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

In general there is uncertainty about the area for this question in Danish law. Several parties have questioned if Denmark has transposed this part of the Data Retention Directive correctly.

---

41 Danish Ministerial Order on Data Retention, section 8.

Only that the providers must comply with the provisions in the Act on Competitive Conditions and Consumer Interests in the Telecommunications Market, cf. question 26.

As far as I am informed there is no general technical or organisational measure that has officially been adopted by the government or the competent regulatory authorities.

It has not been possible for me to find any information on this matter.

a) no data are retained beyond what is permitted?

It is not possible to access this information in public

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

It is not possible to access this information in public

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

It is not possible to access this information in public

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.

It is not possible to access this information in public.

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

The statistic information from the Danish government about the Data Retention Directive illustrates that there have been interception of communication older than the 12 months.[42]

The information is stored for billing for 5 years. According to the Telecommunication Industry the retention data and the billing data are almost

[42] http://www.ft.dk/samling/20081/almdel/reu/bilag/608/700980.pdf

identical. It is possible for the police to access data older than 12 months if the data exists. The legal basis is Administration on Justice Act and its rules on interception of communication.

The Ministry of Justice finds that the Ministerial Order on Data Retention do not contain provisions on the provider's obligation to delete data. The obligations follow from the Ministerial Order on the Provision of Electronic Communications Networks and Services and comparatively the Act on Processing of Personal Data. According to the Ministerial Order on the Provision of Electronic Communications Networks and Services that providers of public communications networks and communication services must ensure, that traffic data regarding subscribers or users must be deleted or anonymised when they are no longer necessary for the delivery of the communication. Though it is allowed for a provider to store traffic data for certain purposes, including billing and for fulfilling obligations pursuant to the Ministerial Order on Data Retention.

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)?

It is not possible to access this information in public.

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

It is not possible to access this information in public.

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 Data Protection Authority has the authority in relation to data retention in Denmark. However, the Data Protection Authority do not have authority to make inspections on location on the providers.

According to the act on Processing of Personal Data the Personal Data Protection Authority has got competence to inspection regarding private controllers, including private providers of telecommunications networks, in the cases on processing of personal data that needs preceding permission[43]. Registration and storage of information on traffic data are not covered by the requirement of permission in the Act on Processing of Personal Data.

According to the Act on Processing Personal Data the authority of the Data Protection Authority in relation to the Ministerial Order on Data Retention include investigations launch by the Data Protection Authority or after complaint from a data subject. The Data Protection Authority ensures that the processing is in

[43] Danish Act on Processing of Personal Data, section 50.

accordance with the Act on Processing of Personal Data. In these situations the Data Protection Authority can demand any information of importance for its activity.

The National IT and Telecom Agency in Denmark is the authority of compliance with the provisions in the Act on Competitive Conditions and Consumer Interests in the Telecommunications Market, section 15. According to these provisions the providers of electronic communication networks and communication services to end users ensure that the technical equipment and technical systems used by the provider are designed so that the police can intercept communication.

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?

It is not possible to access this information in public.

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.

Danish Ministerial Order on practical support of providers of electronic communications network or communications services to the police regarding interception of communication (24-hours point of contact). The providers of electronic communication networks or electronic communication services to end users must establish a 24-hours point of contact. This point of contact must at any time assist the police regarding initiation of a interception of communication.

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?

Cross-border requests must also fulfil the provisions in the Administration on Justice Act on interception of communication. The police must submit the request to the court within 48 hours.

I refer to incoming requests. The district court.

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).

Denmark was the first country in EU to adopt national legislation transposing the data retention directive into national law.

Public debate on the Danish transposition of the Directive of Data Retention was intense. Political parties in the parliament which not a part of the government has been very sceptical. The situation in question 49 is very representative for the debate.

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)?

Airline companies are imposed to register and store data for 1 year. The data must include passenger data and data on crew member on planes arriving to and departing from Denmark.

The obligation follows from the Danish Air Traffic Act section 148a which was included in the second terror packet. The SIS can request the PNR data to be handed out. The Airline Companies must hand over the data as fast as possible and without undue delay.

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.

The Ministry of Justice has published statistics from 2008, where 450.000.000.000 data postings in Denmark were retained. This means that approximately 82.000 data postings on every Danish citizen are retained every year. Out of 450.000.000.000 data postings there were only interception in 3.483 data postings. And only 134 interventions concerned registered internet sessions and e-mail communication.

Besides this case no one seems to really care in Denmark.

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?

The Danish workers Union for IT-professionals made a CD with a computer program that circumvented retention of data. The CD made it possible to circumvent surveillance and censorship when surfing the internet.

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?

As mentioned above both the rules in the Administration on Justice Act section 786, para. 4 and the Ministerial Order on data retention came into force on the 15th of September 2007. In the first terror package there was a provision that the rule in the Administration on Justice Act section 786, para. 4 should be revised in parliamentary session 2005-2006. The second terror package changed this provision so that the rule in the Administration on Justice Act section 786, para. 4 should be revised in parliamentary session 2009-2010 because there was no experience with the rule, since it had not yet entered into force.

In February 2010 the Ministry of Justice published a bill to a public enquiry. The bill contained a provision that abolished the rule about revision on the provision on data retention in the Administration on Justice Act section 786, para. 4.

The Ministry of Justice argued that it had obtained statements from the Director of Public Prosecutions, the National Commission of the Danish Police and The Danish Security and Intelligence Service regarding the practical experiences on the Administration on Justice Act section 786, para. 4 and the Ministerial Order on data retention. These authorities had informed the Ministry of Justice that the data on telecommunication, retained pursuant to the Ministerial Order on data retention, in a wide number of cases had been significant or crucial for the investigation and legal proceedings of serious crimes, including cases on murder, terror, gang-related crimes, drug crimes, home robberies and sexual abuse of children. For those reasons they strongly argued against any changes in the obligation to retain data on telecommunication according to the Administration on Justice Act.

The Director of Public Prosecutions and the National Commission of the Danish Police stated that there could be a need for a longer retention period and retention of more types of data. The Director of Public Prosecutions furthermore suggests that nearer considerations should happen in the light of the EU revision on the Data Retention Directive. The Ministry of Justice agreed with The Director of Public Prosecutions and the National Commission of the Danish Police.

The National Commission of the Danish Police states that the National IT-investigation Center (NITEC). This is an internal police unit used the data retained pursuant to the Ministerial Order on data retention, and that these data often had been crucial for the detection of specific cases, including cases on sexual abuse on children, grooming and hacking.

The Danish Security and Intelligence Service informed that they were using the retained data significantly especially regarding investigations in the area of terror. Informations on telecommunication had been used for the disclosure of terror relations in Denmark and other contries.

Some of the statements from the public hearing were very dissident with the Ministry of Justice.

The Danish Institute for Human Rights and the Telecommunication Industries Association in Denmark pointed out that The Ministry of Justice had not obtained statements from other relevant authorities or companies, including the relevant providers or the Data Protection Authority, who inspects and controls obligations in relation to the retention of data.

The Danish Institute for Human Rights found that the possible consequences for the relevant providers or in relation to privacy, including the Danish transposing of the security rules in the Directive, was not evaluated or had been a part of the decision on abrogate the provision on revision in the Administration on Justice Act. The bill does not contain statistic information on the extent of access to the retained data. This information have been published later on, cf. question 47. The Danish Institute for Human Rights does not find the evaluation of the Danish Data Retention Law balanced since there are no information on the negative consequences in relation to the relevant providers and the right to privacy. Previously The Danish Institute for Human Rights had expressed concerns regarding the Danish transposing of the Data Retention Directive especially the security guaranties in article 4, 7 and 9.

The Telecommunication Industries Association in Denmark also pointed out that the special Danish obligation to retain data on internet sessions that goes beyond the Data Retention Directive entailed that the Danish providers had higher expenses in relation to retention of data.

The Danish trade union for IT professionals (PROSA) had the view that the foundation for data retention was changed because there was a much broader foundation, than originally intended, had originated. The original foundation for retention was the fight against terror, but today the use of the retained data also include organised crime etc.

PROSA asks for information on the retention of sensitive data about the citizens. It is not clear if there already has been unauthorised access to retained data. However, no matter what the data represent a risk of a new kind of crime, where data of the citizens could be misused by others. Worst case the abuse of retained data could be seen as a bigger danger to the citizen and the society than other criminal actions being prevented by the data retention legislation.

PROSA had the opinion that criminals or terrorists without any greater difficulties could communicate on the internet without retention of data. The legislation then would have effect in relation to citizens who did not on them selves protect their behaviour on the internet. PROSA did not find the legislation balancing because the retention had impact on every citizen who used the internet and telephony – which means almost every inhabitant in Denmark. The Danish citizens had the right to privacy and this right was being violated by the data retention legislation.

PROSA wanted the Ministry of Justice to consider if it was prudent to continue retention of data well aware the big risk of misuse.

Subsequently, the Ministry of Justice changed the bill. The revision of the provision on data retention in the Administration on Justice Act section 786, para. 4, was not abolished but postponed to the parliamentary session 2011-2012. Then the evaluation of the Data Retention Directive could be included in the considerations about the revision on the provision in the Administration on Justice Act.

C. National constitutional/legal framework

I. Dimension 1 (State – citizen)

50. Which national fundamental rights protecting privacy, personal data and the secrecy of telecommunications do exist in your country? Are there any other fundamental rights granted to citizens that could be affected by data retention (e.g. freedom of expression and information/freedom of the media, freedom of thought, religion/belief and/or conscience, judiciary basic rights, freedom of profession in cases where the confidentiality of communication is essential etc)? Do the fundamental rights mentioned result from the constitution, from other legal acts or from case-law? Please describe the scope of protection of these fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law[44] – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a specific reason?

According to the Constitution the dwelling shall be inviolable. Any breach of the secrecy shall not take place except under a judicial order, unless particular exception is warranted by statute.

Danish Constitution section 72:

"The dwelling shall be inviolable. House search, seizure, and examination of letters and other papers, or any breach of the secrecy that shall be observed in postal, telegraph, and telephone matters, shall not take place except under a judicial order, unless particular exception is warranted by statute."

The data retention has not really been discussed in relation to the Danish Constitution and especially the provision on the dwelling shall be inviolable. The discussions are about the accordance with ECHR article 8.

There are not any other fundamental rights granted to citizens that could be affected by data retention.

---

[44] 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).

The fundamental rights just mentioned result from the constitution and from other legal acts.

The Danish constitutional law (section 72) only deals with telegraph and telephone matters. It has not been dealt with in constitutional law which data there are considered as telecommunication content.

The Administration of Justice Act contains the provisions on interception of communication and that there must be specific ground for the interception and that the interception fulfil the principle of proportionality.

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?

Any breach of the secrecy shall not take place except under a judicial order, unless particular exception is warranted by statute.

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

There are no rulings on the legal acts transposing the Directive.

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

The national (constitutional) law do not safeguard an *absolute* limit as to the maximum degree to which public surveillance measures *collectively* may restrict fundamental rights. An assessment/balance of interests has to be carried out in each individual case.

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

No, not at national (constitutional) level.

II. Dimension 2 (State – economy)

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

(constitutional) law? Where are the limits to such restrictions according to national (constitutional) law?

The retention obligation do not restrict any fundamental right (e.g. professional freedom) protected by national (constitutional) law vis-à-vis the obligated parties.

The question has not really been discussed in academia.

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)?

National law does not allow to draw on private actors for the purpose of law enforcement or any other purpose of data retention.

Mail companies and providers of electronic communications network or communications services are incumbent on accomplishing the police when intercepting communication. The companies must establish tapping of phone calls and deliver information on telecommunication records and extended telecommunication records. The rules are not specific for data retention but general for interception of communication.

The Administration on Justice Act contain a rule that empower the Minister of Justice to set rules on reimbursement of costs when mail companies and providers of electronic communications network or communications services are assisting the police in intercepting communication.[45] The Minister of Justice has not made use of the empowerment so far.

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

See question 28. Yes

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 ECHR is transposed into Danish legislation as an act. The constitution is above the Danish act transposing the ECHR in the legal hierarchy.

This means that a 'normal' Danish law and the law transposing the ECHR (ECHR-law) are at the same level in the hierarchy of norms. According to the Lex posterior principle a Danish law adopted later than the ECHR-law would in principle be ahead

[45] Danish Administration on Justice Act, section 786(8).

of the ECHR-law. But in practice it would be unthinkable that the legislator intentional would legislate against ECHR. Danish Law contains the so-called rule of interpretation and rule of assumption which entails that the courts will interpret the Danish law in accordance with ECHR.

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?

If the Directive had not been transposed into national law on the 15th of September 2007 it would have had direct effect.

Only the provision that confers a specific right for the citizen to base his/her claim on (in accordance with ECJ jurisprudence.

In order to transpose a directive into Danish law it must first be examined if the state of the law is in accordance with the provisions in the directive. This was partly the case with the Directive on Data Retention, because the provision on data retention could be found in the Administration on Justice Act even though the provision had not been but into force. Directives can also be transposed in to national law in ministerial orders.

No, that will be decided on a case to case basis. When implementing the Data Retention Directive it was first intention to do the implementation only by a ministerial order but as mentioned above in question 13 the implementation was done by an Act and a Ministerial Order

60. Does national (constitutional) law limit the possibility of your country to transfer national sovereignties to the European Union, or does it limit the possibility for the EU to exercise competence already transferred in cases where this would be in conflict with national (constitutional) law?

The Danish Constitution limits the possibility to transfer national sovereignties to the European Union.[46] This was the question in the Danish Maastricht-case which was a Danish counterpart of the German Maastricht-case from BVerfG.[47]

A number of Danish citizens brought charges against the Danish Prime Minister. They claimed that the Danish accession to the Treaty of Maastricht was in conflict with section 20 in the Danish Constitution. The citizens claimed that it was not delegation of sovereignty 'to such extent' as stated in section 20 of the Danish Constitution. The Danish Surpreme Court found that article 352 (Lissabon) must be understood so that the intended legislation act must be within the borders of the function of EU. One must take that interpretation of article 352 (Lissabon) even

46 The Danish Constitution, section 20.

47 BVerfGE 89, 155 Maastricht.

though the provision was interpretated more wide before the change of the Treaty. The Danish Courts must consider an EU legislation act or a EU rule based on ECJ case law inapplicable in Denmark, if the exceptional situation should occur that it can be proven with appropriate certainty that the legislation act or the rule is based on a application of the Treaty that is outside the delegation of sovereignty in the Danish Law of Accession.

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 Ministry of Justice is the responsible ministry in relation to data retention in Denmark. The Ministry of Science, Technology and Innovation also plays a part in relation to the technical parts of data retention. The National IT and Telecom Agency is also relevant in relation to pure technical measures.

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

It is only possible to get access to retained data in accordance with the provisions on interception of communication in the Administration of Justice Act.

IV. Assessment of the overall situation

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

In my view Denmark could learn a lot from transposing the Data Retention Directive, or lack transposing, in the other EU countries. The Ministry of Justice found the Danish transposing in accordance with the provisions in ECHR article 8 back in 2002 when the provisions on data retention were inserted in the Administration on Justice Act and they still think that this is the case.

From a fundamental point of view it is problematic that the provision on data retention was inserted into the Administration on Justice Act back in 2002 and put into force in 2007.

As it might appear from this questionnaire is it also very difficult to use all the different and relevant provision in relation to data retention because they can be found in many different acts and ministerial orders.

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

Denmark

Associate professor Charlotte Bagger Tranberg, ph.d., Aalborg University

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*?

No, national (constitutional) law does not provide a right to communicate anonymous.

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?

In September 2010 the Danish Ministry of Justice published a report on the experiences with the legislation on anti-terror package I from 2002 and anti-terror package II from 2006. In this report it is stated that the Ministry of Justice has formed a working group which must give advice on a possible solution on user registration on prepaid cell phone cards, internet cafes, free hot spots and internet access in public libraries. The working groups must examine and evaluate the technical possibilities for registering of this kind of information, including experiences from other countries, clarify economic and administrative consequences and involve the telecommunication industry in the process.

The document has not yet been published (august 2011) and since there has just been called for election in Denmark it is not likely to be published in the next few weeks. The Danish newspaper "Politiken" has referred to the main point of the

document in June 2011. Hereof it emerges, that all users of open internet connections must use a personal code or be registered in another way in the future. This gives the police an opportunity to discover who the users communicate with or which home pages they visit.

Danish law already contains rules similar to the rules on quick freeze in the Cyber Crime Convention. According to the Administration of Justice Act paragraph 786a – and as a part of an ongoing investigation - the police can give internet service providers an order to preserve electronic data, including traffic data, important to the investigation. Orders on data preservation can only include data retained when the order is given. The aim of the provision is to ensure, that internet service providers can be ordered — to store *existing* data in a period up to 90 days, and to ensure that the data – under the right conditions – can be handed over to the police later on. According to the bill of the provision transmission of preserved data must still fulfil the requirements in the Administration of Justice Act section 781 (1-3) and section 804(3). According to transmission of content data and traffic data it must be demanded that there is an investigation of an offence that can be punished with jail in six years or more. Danish law does not contain rules on prospectively data preservation.

When the rules on data preservation were adopted back in 2004 there was no discussion on the relationship between data preservation and data retention.

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?**

   Citizens and undertakings are not in generally obligated to coorporate with public authorities in the detection, investigation and prosecution of criminal offences.

   ISPs are only obliged to retain data in relation to the rule on data retention. Before the rule on data retention was adopted it was a problem, that the providers did not all retain the same kind of data for the purpose of billing and accounting, so that the data existed if the police should need it.

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?**

   According to the Administration of Justice Act section 170 defence lawyers, mediation lawyers and lawyers in general can refuse to testify. The court can order

mediation lawyers and lawyers – but not defence lawyers – to testify, when the statement is considered to be crucial to the outcome of the case. If secrecy is essential the court can decide that the testimony shall not contain information that is assigned to duty of confidentiality.

It is unclear whether or not these rules include retained data, but they probably do.

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?**

   There are no specific rules on where or how the requested data must be stored by the bodies that obtain them. That means that the general rules on security in relation to processing personal data in the Danish Act on Processing of Personal Data paragraph 41 are being applied. According to paragraph 41(3) the controller shall implement appropriate technical and organizational security measures to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Danish Act on Processing of Personal Data.

6. **Are there any official statistics or otherwise available information on the transmission of retained data to the entitled bodies (number of requests, data categories, time period between storage and request)? If so: please attach this information or give a brief summary and indicate their source.**

   There are no other official statistics than the ones send to EU in 2008 and 2009. The numbers can be found in COM(2011)225. In relation to the data send to EU there is data retained longer than one year – it is because the data is also retained according to other rules – billing and accounting.

B. Country-specific questions

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

   There has not been any public debate on the constitutionality of the data retention regime in Denmark.

   The Danish legislation on data retention does not contain specific rules as the rules in 2006/24/EC after which the data retention directive shall not apply to content of electronic communication, cf. article 1(2) and article 5(2).

   But at the same time in must be noted, that the provision in section 72 in the Danish constitution is narrower that the provision on the right to privacy in ECHR article 8.

   Section 72 in the Danish Constitution protects the content of communication, and since the Danish rules on data retention include session data, the rules on data

retention are not in accordance with the constitution. The discussion on this issue has never been dealt with.

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?**

   In principle yes, but the special Danish rules on retention of session data is not completely in accordance with the secrecy of correspondence, cf. the answer to question 7.

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

   The Danish Government did not focus on the impact on the principle of proportionality when adopting the Danish rules on data retention. As mentioned in the first questionnaire, it was implicit provided that the rules complied with proportionality rules.

   The Danish Constitution does not contain a provision similar to ECHR article 8 (2).

10. **Is the limit that the "Danish Maastricht ruling" has set with regard to the use by the EU of the national sovereignties conferred to it in any way binding for Danish representatives 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?**

    No.

11. **Please describe the following safeguards of the rule of law in detail:**

    - **catalogue of criminal offences for the investigation and prosecution of which the use of retained traffic or location data is permitted,**

      I can not answer this question more precise than question 16 in questionnaire I.

    - **requirement of a court order prior to the data request: please describe the steps the entitled body has to take in order to obtain the court order. What will the court examine before taking a decision on whether or not to issue the order?**

      I can not answer this question more precise than question 17 in questionnaire I.

    - **role and tasks of the lawyer appointed to the aggrieved party.**

      I can not answer this question more precise than question 18 in questionnaire I.

12. **Please describe the steps the entitled body has to take in order to obtain a court order prior to the data request. What will the court examine before taking a decision on whether or not to issue the order? Which cases are to be regarded as "emergency cases" so that access to the data may be sought by the Prosecutor or the Investigating Judge? Is it necessary to have a court decide on the lawfulness of the access after the emergency situation is over?**

    I can not answer this question more precise than question 17 in questionnaire I.

    But it must be underlined that the permission is given in most cases when the word 'terror' is being mentioned. Some researchers has commented this issue in the press and mentioned that it is not a real barrier in relation to interception on communication.

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

    No, there are no rules preventing the same data from being retained more than once.

14. **As regards your answers to questions 38 and 39 of the first questionnaire: Does Danish law provide for rules on the transfer of personal data to third countries that correctly transpose the provisions laid down in Chapter IV of Directive 95/46/EC?**

    Yes, they are the same as in the provisions in the directive.

15. **Are there any (data retention-specific or general) provisions that allow the bodies entitled to obtain access to the data retained to *transfer* these data, once obtained, *to other authorities* for their respective purposes? If so, please describe the requirements that have to be fulfilled for such transfer, and how data exchange between them is effected in practice.**

    No.

16. **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?**

    No.