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

The Netherlands

Mr. Drs. J.V.J. van Hoboken

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

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

I. Legal provisions

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

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

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

Yes, they have been transposed in July 2009 and entered into force on 1 September 2009.

- ***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)?

/

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.**

   No, there is no English text available of the Dutch data retention law.

   The Dutch law is called (short ttile): 'Wet bewaarplicht telecommunicatiegegevens', Staatsblad 2009, nr. 333, available online at: https://zoek.officielebekendmakingen.nl/stb-2009-333.html

   The long title of the law is 'Wet van 18 juli 2009 tot wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG'.

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

   The transposition law has been officially adopted on 18 July 2009. The provisions have entered into force on 1 September 2009, by Royal decree of 25 August 2009, Staatsblad 2009, nr. 360.

   Notably - this goes to the political debate about the law- , the Dutch Government - at the time of the debate about the adoption of the law in the Senate - promised the Senate to bring forward a new legislative proposal to lower the retention period for internet traffic data to the minimal 6 months. This promise made it possible for the proposal to receive enough votes in the Dutch Senate, which is not allowed to amend laws. The Senate had been highly critical of the necessity of the proposed

law‘s interference with the right to private life as enshrined in Article 10 of the Dutch Constitution and Article 8 ECHR. A year later, in 2010, political realities have changed (the Dutch government coalition fell in early 2010) and the retention period for all related data will stay 12 months for now.

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

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

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

   The legislative act contains the core data retention provisions and stipulates the data to be retained in an annex to the law (it is considered part of the law). The core data retention provisions include:

   - The obligation for public electronic communication service and network providers to retain the set of data as mentioned in the annex for a period of 12 months (Article 13.2a Dutch Telectommunications Act). In the provision itself, the retention obligation is explicitly extended to data relating to unsuccessful call attempts if traffic data relating to those attempts is already generated and registered.

   - An annex defining the data to be retained. (annex to article 13.2a Dutch Telecommunications Act).

   - An exception to the usual restrictions on the legitimate grounds service and network providers can have for processing subscriber data and traffic data, to allow for data retention which is necessary in view of the interests of national security, the prevention, investigation and prosecution of crimes (Article 11.13. Dutch Telecommunications Act).

   - An obligation to respond without delays to legal requests by law enforcement authorities (on the basis of existing legal provisions in The Dutch Criminal Code for identifying data or traffic data) or the Dutch national security agencies (on the basis of provisions in Dutch national security law) to get access to the retained data (Article 13.2b Dutch Telecommunications Act).

   - An obligation to provide for the security and confidentiality of the retained data (Article 13.5 Dutch Telecommunications Act), and in particular:

- to guarantee the integrity of the retained data, to prevent the loss or modification of retained data,
- to prevent unauthorized access
- to ensure the (possibility of) deletion of the data after the retention period has elapsed
- to treat the data to be retained with the same security measures as the normal data in the network.

- An obligation on the Dutch government to provide an evaluation, each three years, of the effects and effectiveness of the data retention laws (Art 13.9 Dutch Telecommunications Act).

In line with legislative practice in the Netherlands, the Act allows and anticipates for lower rulemaking through administrative decrees (requiring the most official form of lower rulemaking) in the following areas:

- More precise stipulation of the data to be retained (Art. 13.4.3) (The annex is similarly general as the list of data as mentioned in the Directive, leaving open many questions of practical implementation and application. There has been criticism of not precisely defining the data to be retained in the law itself by the Dutch data protection authority in its advice on the legislative proposal. This advice is available in English and contains valuable factual data.[1])

- More precise stipulation of how service and network providers should lawfully respond to legal requests by law enforcement and national security agencies, how they should keep the data available, and how statistical data should be collected. (13.4.4 Dutch Telecommunications Act) The fact that the gathering of statistical data has not been implemented leads to the conclusion that the directive has not been fully transposed in this regard. In addition, it has been noted that this provision (Article 13.4.4.) also allows for an administrative decree that would require centralized storage of the retained data.

- More precise rules on how to guarantee the security and confidentiality of the data to be retained (Art. 13.5.4 Dutch Telecommunications Act). There was and is already such an administrative decree in force with detailed obligations relating to the security and confidentiality of electronic communications data.

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,

[1] See Dutch DPA, CBP Opinion on Implementation of the Directive on Data Retention, 22 January 2007, available online at http://www.dutchdpa.nl/downloads_adv/z2006-01542.pdf.

2002/21/EC and 2002/58/EC) that have also been legally defined in national legislation?

Yes, all the terms as defined in art. 2 para. 2 of Directive 2006/24/EC have been defined in the Dutch law. They have been defined in the legislative act ('Wet bewaarplicht telecommunicatiegegevens') itself and are identical to the definitions in the Directive. No specific new legal terms, other than those mentioned above, have been created in the context of the transposition of the Data Retention Directive.

Dimension 1 (State - citizen)

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

The data to be retained, according to the annex to the law as mentioned in the answer to question 7, are precisely the list of data as stipulated in Article 5 of the Directive. In addition, the Dutch law anticipates the retention of location data during (and not only at the start of) communications, but as regards IP communications there it is not yet fully clear what data should and will be kept in practice. (Annex to article 13.2a Dutch Telecommunications Act.)

The Dutch law provides that data relating to unsuccessful call attempts have to be retained if these data are already generated and registered (Article 13.2a Dutch Telectommunications Act).

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

The retention of content data is not specifically regulated, but falls under the guarantee of confidentiality of communications, which is constitutionally protected (Article 13 Dutch Constitution). There are legal wiretapping powers, that make it possible for law enforcement and national security agencies to have electronic communications content retained (in specific cases) and to access it. Article 13.1 of the Dutch Telecommunications Act contains the obligation that all public electronic communications services ensure they can wiretap their services. Article 13.2 of the Dutch Telecommunications Act contains the obligation to respond to legal wiretapping requests by law enforcement or national security agencies. Law enforcement wiretapping powers are stipulated in Artt. 126m and 126t of the Dutch Code of Criminal Procedure (Wetboek van Strafvordering). The National Security Agency wiretapping power is stipulated in Article 25 of the Dutch National Security Act (Wet op de inlichtingen- en veiligheidsdiensten).

In line with the e-Privacy Directive (2002/58/EC), the Dutch telecommunications law contains a legal regime for the lawful processing of customer records and traffic and location data by electronic communications service and network providers. This regime is codified in Chapter 11 of the Dutch Telecommunications Act. The regime consists of the obligation to make anonymous subscriber and traffic data after these data are no longer necessary for the transport of communications with the exceptions of when the processing is necessary to

- for itemised billing and interconnection payments;
- conduct market research and sales activities relating to electronic communications services;
- the provision of value added services.

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

For the prevention, investigation and prosecution of crime and for national security purposes. The Dutch Code of Criminal Procedure (Section 1.IV.7 and Section 1.IVa.7 title 1.V) and the Dutch national security act (Article 25-29) contain rules about the way in which access to the retained data can be obtained by law enforcement and national security agencies.

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)?

No, there are no specific rules for the retention and transmission of traffic and location data that could be considered particularly sensitive because of who or what they relate to, such as traffic data relating to the communications between lawyers and their clients.

There are some special rules with regard to the wiretapping and subsequent processing of the wiretapped content of the communications themselves. These rules are politically debated and subject of litigation, see e.g. Rb The Hague 15 March 2005, Rb Amsterdam 20 December 2007 (Hells Angels). Legal wiretapping powers in Dutch law do not contain specific rules for the treatment of wiretapped communications in which trusted parties such as a lawyer participated. But, in principal, such communications, if they happen to be wiretapped, have to be deleted (art 126aa Dutch Code of Criminal Procedure).

"Seen together, your responses to question 12 and 50 say (according to my understanding) that in the Netherlands, at present, there is no national law excluding the traffic data of certain communications that are considered "sensitive" (such as

those described in question 12) from the obligation to retain them AND to hand them over to public authorities, although the content itself might be considered to be "sensitive". At the same time, there have been some discussions on the compatibility with fundamental rights of data retention as a whole for possibly interfering with the right to the confidentiality of communications, but this has not been object of a court case yet. Is this understanding correct?"

Yes, this is the case.

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.**

The retention period is 12 months.

As mentioned above, the Dutch Government promised to lower the retention period for internet traffic data to the minimal 6 months. The reasons for this were the proportionality from the perspective of fundamental rights and the more challenging context for technical implementation in the Internet context. In particular, the necessity of longer retention than minimal (6 months) was not considered to be convincingly established for Internet traffic data. It is likely, however, that a new Dutch government will not live up to this promise and the retention period for all related data will stay 12 months.

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)?**

There are explicit provisions that allow access for law enforcement agencies and national security agencies in section 1.IV.7 and Section 1.IVa.7 title 1.V) and in the Dutch national security act (Article 25-29).

The Dutch Code of Criminal Procedure contains a range of legal powers to access retained data (electronic communications data and identifying data) by law enforcement agencies.

Most commonly, a request for electronic communications data will be based on Article 126n of the Dutch Code of Criminal Procedure. This Article contains the power for the public prosecutor to request access to electronic communications data when those data are needed for an investigation into a specific crime. There is a relatively low threshold for the kind of crimes the investigation has to relate to (Article 67 Code of Criminal Procedure). (For details, see the answer to question 16)]. Notably, the requested data does not have to relate to a suspect, it simply needs to be in the interest of the investigation to obtain the data.

For identifying data (subscriber data) the threshold is lower. Normal law enforcement (police officers) can request access to those data on the basis of Article

126na of the Code of Criminal Procedure. In practice, access to those data takes place through the CIOT, a central clearing house for subscriber data.

Article 126hh Code of Criminal Procedure contains the most far-reaching power to request personal data held by public bodies or private parties and includes the possibility to data electronic communications. It stipulates the legal power to request access to a complete file or parts of a file (e.g. a file of retained traffic or location data).It can be used by the public prosecutor if this is needed in the interest of an exploratory investigations into terrorist crimes. The provision was adopted to allow for datamining in the context of investigations into terrorist crimes. Article 126hh requires authorisation by a judge. The legal term 'file' in article 126hh Code of Criminal Procedure is the same as the term file in the Privacy Directive (95/46/EC). The provision allows for a request of a complete file or piece of a file that is easily separable from the complete file; the request does not have to be restricted to specific persons. The provision can only be used in the context of a preliminary investigation into terrorist crimes. An amendment to exclude the communications data stored as a result of the Dutch data retention law from the scope of Article 126hh did not attract enough votes in the Parliament to be adopted.

Article 28 of the Dutch National Security Act (Wiv) contains the power for the national security services to request electronic communications data. Article 29 of the same act contains the power to request subscriber data.

The status of access to retained data by private litigants or other public agencies and bodies is excluded in the legislative act but Dutch tort law may still be argued to contain an obligation to provide electronic communications data. See also answer to next question.

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)?**

Law enforcement agencies: for the prevention, investigation and prosecution of crime.

Intelligence and National security.

Access for private litigants: The legislative memorandum excludes access for others than law enforcement and national security agencies. Over the last 15 years, Dutch law has developed (through case law) a ground for obtaining access of electronic communications data for private litigants that is in tension with this exclusion. It has been accepted in case law relating to illegal or unlawful acts on the Internet that general tort principles include an obligation for electronic communications providers to provide data that can identify that source of a claimed wrongdoer. It remains to be seen how these standards will develop after the entry into force of the Dutch data retention law. As a result, in practice, Dutch electronic communications

providers provide identifying data to private litigants in individual cases, if there is sufficient proof for an alleged unlawful act by the respective subscriber and there are no alternative means to identify him or her.

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)?

Generally, the retained data can be accessed by law enforcement and national security agencies on the basis of provisions that had already been enacted by the Dutch legislature. For specific provisions, see the answer to question 14 above. No specific restrictions to these existing powers have been imposed in the context of the data retained as a result of the electronic communications data retention. There is also no requirement of last resort to access retained electronic communications data. The Dutch government has emphasized a number of times that the transposition law would not change the conditions to gain access to electronic communications data.

Law enforcement agencies have specific legal powers (See answer to question 14) to request access to subscriber data and traffic or location data. Access to data, for any category of data, is not restricted to data relating to a suspect. The lowest threshold applies to identifying (subscriber data). Normal police officers can legally obtain access to these data if they are relevant to an investigation of a crime. For traffic and location data, involvement is required of the public prosecutor's office and there is a restriction for the types of crimes the investigation has to relate to. Although this restriction is sometimes referred to as a restriction to more serious crimes, in reality this restriction is not very meaningful. The list of crimes (Article 67 of the Dutch Code of Criminal Procedure) includes all crimes with at least a maximum sentence of 4 years as well as a long list of other crimes. As a result, it is undoable to even produce a list of all crimes that are covered. It suffices to state that there are a range of relatively trivial crimes that are covered by this provision, such as simple theft, the handling of stolen goods regardless of the good involved, and even the use of dogs as a pulling power. Hence, this threshold is incomparable to the serious crimes listed in Council Framework Decision 2002/584/JHA, or the Schwere strafftaten in German Law (§ 100a (2)).

Notably, relatively new legal provisions that allow for bulk requests and data mining in the context of preparatory investigations into terrorist crimes (art 126hh. WvSv) by law enforcement agencies, are also applicable to the data retained. An amendment to exclude the retained data from their applicability was not adopted in parliament

National Security. Access to the data has to be legitimated on the grounds that it is necessary for the general intelligence and national security agency to fulfil its tasks as specifically defined in Dutch law. The tasks of the national security agency and the military intelligence agency are defined and delineated in the Dutch National Security Act, Artt. 6, 6a, 7, 7a. As an example, the Dutch general intelligence and security agency has the task to investigate persons or organizations that because of the goals they pursue or because of their activities give rise to serious suspicion that

they are a threat for the existence of the democratic legal order, or the security or for other fundamental interests of the state (Article 6 (2) of the Dutch National Security Act (Wiv)).

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?

No, there is no need for law enforcement agencies to obtain a court order to access historic electronic communications traffic and locations data. National security agencies can also access the data without having to fulfil very strict criteria, as apply to certain other investigative powers. There is also no need to hear or involve the aggrieved party beforehand.

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?

There is a general obligation in Dutch criminal procedural and national security law to notify the party whose data has been accessed by law enforcement and national security agencies.

In the context of access to electronic communications data, this obligation (article 126bb of the Code of Criminal Procedure) does not apply to identifying data (see Article 126na (3)) but only to traffic and location data. The notification, when required, should take place afterwards. Notification is not needed if it cannot reasonably be required. In practice, notification seldom or never happens. There have been several debates in Dutch parliament about the lack of compliance with the notification obligation.

There is a similar but more narrow notification requirement in the context of national security agencies and it contains a more permitting exception. First, the notification requirement for the national security agencies (Article 34 of the Dutch National Security Act, WiV) does not apply to legal requests for electronic communications data or subscriber data. It does apply to wiretapping. Second, in practice, notification has never taken place in this context, as a recent report from the official agency overseeing the national security agency showed.[2] The government has recently stated it wants to abolish the active notification obligation in the national security context and replace it with the obligation to respond to requests for information.

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

See also the answer to question 18.

---

[2] See Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, 'Onderzoek naar de rechtmatigheid van de uitvoering van de notificatieplicht door de AIVD', report nr. 24, 2010.

There are general rules, on the basis of Directive 95/46/EC, that give every person a right to access his or her personal data in the public and private sector (article 35 of the Dutch Data protection act). The right to gain access applies to all personal data held by a data controller, which has to respond by providing all the personal data which are processed of the data subject in an understandable format, within 4 weeks after a request has been made, as well as the categories of data, the goals of the processing of the data, the recipients of the data and the origin of data.

This general provision applies to electronic communications service providers, but Law enforcement and national security are not covered by this general data privacy rule. Requests to gain access to data held and processed by law enforcement agencies can be made on the basis of and in accordance with Articles 25-27 of the Law Enforcement Data Act (Wet Politiegegevens). Requests to gain access to personal data held by the national security agency can be made on the basis of and in accordance with Articles 47-50 of the National Security Act.

Articles 25 of the Law enforcement data act provides that the police has to respond to a request for data within 6 weeks, with a possible extension of 4-6 weeks. Article 26 provides that the authorities have to ensure proper identification of the data subject and provides for other minor formalities. Article 27 provides for exceptions to the obligation to provide the personal data to the data subject in case it is necessary to withhold the data because of the proper functioning of the police, the weighty interests of third parties, or the security of the State.

Article 47 of the National Security Act provides that requests by data subjects to the Minister of the Interior about the processing of their personal data by the national security services are responded to in 3 months with a possible extension of 4 weeks. Article 48 provides that data subjects that have gotten access to their data as a result of a request ex article 47 are allowed to add a written statement to their file that they have gotten access. Article 49 provides for a special regime for access to personal data internal to the operations of the national security services for employees or former employees. Article 50 provides for the possibility to request access to personal data by close relatives of deceased data subjects. All requests relating to data that have been processed in the period of 5 years before the request, or data that are still relevant to an ongoing investigation have to be declined (Article 53). Article 55 lists the specific interests of the State and third parties which have to lead to a negative decision on a request to gain access to data.

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?

Article 552a of the Dutch Code of Criminal Procedure, contains a possibility to complain about access to data by law enforcement agencies. This complaint does not bar access and can be made by any interested party (the one holding the data as well as the one(s) to which the data relates).The complaint has to be made at the

court, interested parties are notified and the court decides on the validity of the complaint.

If the complaint is found to be valid the Court's decision provides for a corresponding order. (Hence: If the data has not yet been accessed, no access to the data will be permitted. If the data has already been accessed, the data will probably have to be deleted, but this depends on the specific circumstances of the case.)

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 transposition law contains an obligation to provide for the security and confidentiality of the retained data (Art 13.5 Dutch Telecommunications Act), and in particular:

- to prevent unauthorized access
- to treat the data to be retained with the same security measures as the normal data in the network.

More specific safeguards are provided in a general administrative decree: 'Besluit beveiliging gegevens telecommunicatie', [Decree security telecommunications data]. This decree details a list of technical and organizational measures to be taken with respect to electronic communications data. This includes:

- An obligation to have a security plan, which has to clarify the way in which the provider complies with existing obligations
- An obligation to take a number of measures, including measures relating to employees and employment; access to buildings and physical facilities; proper functioning and security of information processing systems; the ability to prevent and deal with unauthorized access; calamities.
- An annex to the decree with a list of more precise requirements.

(Annex, rough author's translation)

Annex referred to in Article 2, third paragraph of the Decree security telecommunications data

I. General security requirement
There is an officer responsible for overseeing the implementation and enforcement of security. The officer shall regularly carry out inspections and lay down his findings in writing.

II. Personnel security requirements
a. The responsibility for data security is part of the job description of staff responsible for processing of such data.

b. Personnel that has contact with the information and data signs a confidentiality agreement.
c. Only personnel that is responsible for processing the information and data under their job description has access to information and data.

III. Physical security and protection of the environment
a. The information and data are confined as much as possible to a single concentrated area.
b. The area in which information and data are physically present, is properly secured.
c. Physical security is designed so that unauthorized access attempts are detected and that timely intervention takes place.
d. Access to the room where the data or the information is allowed only to duly authorized persons to the extent necessary for their functioning.
e. Entering and leaving the room must be so regulated that it is controlled and later on identifiable at the individual level.
f. Documents in which, or removable media on which the information and data are laid down, are stored in properly secured containers.
g. Persons responsible for maintenance and repair work in the area in which information and data are kept are being supervised by own authorized personnel.

IV. Management of communication and control processes
a. The status / classification of information and data (state secret or confidential) should always be known.
b. Reproduction of information or data is permitted only by authorized persons and only to the extent necessary for the proper execution of the special charge or authorization under the Law on the Intelligence and Security 2002 under Article 13.2,first and second paragraph of the Act or an application under Article 13.4 of the Act.
c. The information or data is not placed outside the normal space, unless this is necessary for the proper progress of the work taking place. In that case, the whereabouts of the information or data is being recorded.
d. The removal and destruction of information and data will take place in an irreversible manner. Of removal and destruction a report is made, a copy of which is to be sent to the competent authority whom it concerns, or an authorized agency.

V. Access security of automated information
a. Access to computerized information systems in which information and data are processed is protected in a sound manner protected, including by means of personal authentication.
b. The logical security is designed in such a way that unauthorized access attempts are detected and that timely intervention takes place.
c. The number of bad password attempts is limited to three. Exceeding the number of bad password attempts results in a definitive block of the account, and can only be removed by the officer referred to in section I of this Annex. The foregoing shall not apply to the system manager, provided that after three bad password attempts a renewed attempt to login can only occur through an emergency set up account and personal authentication for the use of which the official referred to in section I of this Annex must have granted his approval.
d. The computerized system in which data and information are processed, is not left before eaving a (manual or automatic) access control mechanism is provided.
e. All transactions relating to the processing of information and data in the computerized information system si recored at the individual level to enable investigations.
f. Access to the automated information systems is restricted to authorized personnel only.
g. The access rights of users are periodically reviewed.
h. The authorizations of all users is being recorded.

VI. Development, maintenance and repair of automated information
a. Any changes in equipment, software or procedures that protect or can influence the security of the data and information are verifiable, meaning that they are known and evaluated by or on behalf of the vendor as being acceptable.
b. The maintenance of computerized information systems that still provide access to data and information, takes place on location.
c. Notwithstanding subparagraph b, the remote maintenance of computerized information systems is allowed only if it is performed by authorized persons referred to in part II of this Annex, and only at times authorized by the official referred to in section I, a of this Annex, and if there are sufficient safeguards for maintaining the security level for the data and information.
d. Repairs to the computerized information systems in which information and data processing is done takes place on location. This requirement can be waived only if the information and data is deleted and cannot be traced back.

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

This falls under the general laws of processing of personal data by law enforcement agencies, 'Wet Politiegegevens' [Law enforcement data act]. No specific rules have been adopted for electronic communications data.

This law gives law enforcement agencies that access data considerable leeway to keep and use those data for at least a year. As a general maximum limitation on the time the data can be kept by law enforcement agencies, Article 8 of this law provides that data can be processed for 1 year for general police purposes and also after that initial period has elapsed but they should be deleted if their are no longer necessary for law enforcement purposes. If data are deleted they are actually still stored for 5 years (to enable to responses to complaints and to account for activities). The data have to be deleted after those 5 years. (Article 14 Law enforcement data act). As an exception, the law enforcement data act provides for the possibility that stored data can be processed on the basis of renewed grounds (Article 14(3)). The law allows for correlation with other data and, under certain conditions, it allows for data-mining (article 9-11 Law enforcement data act).

Dimension 2 (State – economy)

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

Public electronic communications service and network providers. These are the services that are regulated by the EU Electronic communications framework and the Dutch telecommunications act. As a result, closed and private networks or services are not covered. The Dutch Telecommunications Act uses precisely the same definitions for closed and public as the definitions in the EU Electronic Communications Directives (2002/21/EC).

Public electronic communications network is defined in Article 1.1ee of the Dutch Telecommunications Act (openbaar telecommunicatienetwerk)

Public electronic communications service is defined in Aricle 1.1 ff of the Dutch Telecommunications Act (openbare telecommunicatiedienst)

Web-based communications services offered from abroad such as gmail are considered to be outside of the scope of the obligations as well as internet hosting providers. Internet telephony that is pc-to-pc based and does not use the official number plan is also not covered.

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

No, there are no additional exceptions to retention obligations that would exclude certain public electronic communications service and network providers from data retention obligations, such as for non-commercial service providers or providers with minor turnover. (See also answer to question 23).

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?

For fixed and mobile telephony, the obligations do not seem to give rise to the processing of new categories of data, only the lengthened storage and keeping available in appropriate formats.[3] To my knowledge there are no data available on historical compliance of service providers with the rules as mentioned in the response to question 10 of this questionnaire.

For Internet data, the data categories are not yet adequately defined for practical purposes. There are a lot of questions as to what measures should be taken by different providers. It seems likely that providers of Internet related electronic communications services or networks will have to make changes to be compliant with the new law.

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)?

Art 13.5 Dutch Telecommunications Act contains specific obligations to guarantee the integrity of the retained data, to prevent the loss or modification of retained data, to ensure the (possibility of) deletion of the data after the retention period has

[3] See 'Toelichting bewaring gegevens' [Explanation retention of Data], 29 June 2010, available at http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/richtlijnen/2010/06/29/toelichting-bewaring-gegevens-telefonie/toelichting-bewaring-gegevens-telefonie-10-06-29.pdf

elapsed and to treat the data to be retained with the same security measures as the normal data in the network.

More specific safeguards are provided in a general administrative decree (Besluit beveiliging gegevens telecommunicatie, Decree security telecommunications data). This decree details a list of technical and organizational measures to be taken with respect to electronic communications data. See answer to question 18 for details about the substantive requirements in this decree.

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)?**

    No adequate actual figures are available to answer this question.

    An independent study (VKA) from 2006 estimated the costs for the current implementation (12 month periods, decentralized storage) to be a 75 million EUR initial investment and subsequent 20 million a year. This does not cover the costs to comply with requests to actually access data. The researchers could not base their study on figures showing which data were already readily available (providers did not provide these data), hence they predicted the actual costs to be less. In addition, costs were predicted to go down because of technological advances (e.g. storage capabilities).

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

    The costs for the actual handling of requests for actual data are reimbursed through standard tariffs:

Responding to legal request for identifying data	€ 7,45
Responding to legal request for historic identifying data	€ 7,45
Responding to legal request for historic traffic data	€ 7,45
Responding to legal request to conduct file analysis	€ 29,82
Responding to legal request relating to location labels	€ 29,82
Cooperating with complex queries, not covered above	€ 29,82 an hour

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

No specific formal rules have been enacted to deal with co-operation in the context of data retention. The law does anticipate such further rulemaking through the enactment of administrative decree(s) in Article 13.4.4, but these have not been proposed or enacted.

Generally the co-operation between law enforcement and service providers is shaped by

Criminal procedural law (see the powers as described and listed in the answer to question 14),

Administrative decrees. As mentioned above, existing administrative decrees do not cover data retention data, but amendments are foreseen. Most importantly, the decree supply telecommunications data (Besluit Verstrekking Telecommunicatie) could be amended to cover retained electronic communications data. This administrative decree currently regulates the provision of non-historic subscriber data through the central entity CIOT. (for more details about CIOT see the answer to question 38).

Ministerial regulations. There are rules for the cost reimbursement based on Article 13.6 of the Dutch Telecommunications Act. In wiretapping context there is a ministrial regulation, namely the Regeling Aftappen Openbare Telecommunicatienetwerken en -Diensten.

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.

The data retention law provides has amended the General Law on Economic Crimes which now makes a lack of compliance with the obligations to retain data (Article 13.2a), to respond to legal requests for these data (article 13.2b and Article 13.4), and to provide the security and confidentiality as stipulated (article 13.5), are economic crimes, if purposefully committed, and offenses otherwise.

Compensation by individuals would have to be based on the rules of general tort law as Dutch telecommunications law and the data retention law do not provide for specific ways of redress. Of relevance in this context would be the new data breach notification obligation from the amended ePrivacy directive, but those new rules await implementation in the Netherlands.

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?

The entitled body (to request access to retained data) does so itself.

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

No, there are no regional entities vested with own authority in respect to retention of electronic communications data.

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

The transposition of the data retention directive has not yet led to the adoption or amendment of the rules of co-operation referred to in the question.

The general rules relating to the processing of personal data in the context of law enforcement are applicable. ('Wet politiegegevens', Law enforcement data act,) This act provides the legal basis for the processing of data (including personal data) in the context of the Dutch justice and law enforcement system. It stipulates for which purposes data can be processed, how and from whom data can be collected and to who (other public authorities) the data can and may be provided.

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)?

There is no possibility for foreign agencies to access data held by electronic communications providers directly. In general, requests have to follow the general rules for foreign requests for legal (law enforcement) assistance. Those rules are laid down in Title X of the Code of Criminal Procedural Law (Wetboek van Strafvordering). Those general rules stipulate that requests for electronic communications data have to proceed through the office of the public attorney. See articles 552h and 552i of the Code of Criminal Procedure.

Cross-border exchange of data for law enforcement purposes is also the subject of various treaties, and European Union secondary legislation. The general rules as laid down in Title X of the Code of Criminal Procedure stipulate that exceptions may apply on the basis of such treaties and EU law. See in particular Council Act of 29 May 2000 regarding Mutual Assistance in criminal matters between the Member States of the European Union.[4]

Reports suggest that many requests, in particular in border areas such as with Germany, may be dealt with informally because of the complexity of official procedures.[5]

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 Agentschap Telecom [Radiocommunications Agency], an administrative agency which is an operational part of the ministry of economic affairs for issues related to telecommunication in the broad sense. This Radiocommunications agency is an operational part of the ministry of economic affairs and as such falls under the direct and single authority of the ministry. As the agency states on its website, "*Radiocommunications Agency Netherlands acts as the watchdog, implementer and expert across the entire domain of electronic communication*". [6] They are the primary agency overseeing proper execution and compliance with the law. This agency is also responsible for providing industry guidance and has been actively engaged with the industry to do so in the context of data retention obligations.

Of relevance is also the Dutch Data Protection Authority (DPA), the independent supervising agency overseeing compliance with the data protection act. Only as a matter of funding, the Dutch DPA is part of the Ministry of Justice.

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, there are no lawsuits concerning the legality of data retention law in the Netherlands.

---

4 See http://europa.eu/legislation_summaries/justice_freedom_security/judicial_cooperation_in_criminal_matters/l33108_en.htm.

5 See e.g. http://spl.politieacademie.nl/vereenvoudigde-procesgang-rechtshulpverzoeken-is-haalbare-kaart/tabid/603/Default.aspx

6 See Radiocommunications Agency, http://www.agentschap-telecom.nl/english.

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, there are no lawsuits concerning the legality of data retention law at the European level (EU or CoE).

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 storage of data is decentralized (at the providers) but it is possible to require centralized storage by administrative decree at a later stage.

Notably, non-historical identifying data of electronic communications subscribers – the storage of which predates the data retention law - are centrally stored through the CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie). CIOT receives daily batches of subscriber data from providers and provides access to such data for law enforcement and national security agencies. The CIOT database is accessed around 3 million times a year, at a growing rate of a around 20%, a seemingly excessive amount considering the Dutch population amounts to only 16 million people. There have been discussions to extend the operations of CIOT to historic subscriber and traffic data, retained as a result of data retention obligations. A business case to do so has been already finalized and is being discussed by relevant actors.

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?

Dutch law and regulations do not provide for specific rules about the possibility to store data elsewhere so this depends on the application of general telecommunications and privacy rules. Providers may take the view that the provision of the service and not the storage or processing of data triggers the data retention obligation and that storage is a matter to organize for themselves effectively. Clearly, providers that fall under the Dutch data retention obligations will at least need to comply with the Dutch provisions if data are stored abroad.

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

a) no data are retained beyond what is permitted?

There is a legal obligation not to do so but if this is actually the case and how this guarantee is met, depends on the provider. In the context of Internet Service Providers, a recent study by the Agentschap Telecom about the state of practical compliance of data retention obligations (the agency mentioned in the answer to

question 35) shows that some of most providers do not consider this a priority yet.[7]

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)?

No court order is required. Technical interfaces, if existing, depend on the providers.

Direct access is possible to non-historic data through the CIOT. There are plans to extend the CIOT database to cover some of the historic data as retained on the basis of the Data retention act.

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

This depends on compliance with the general rules on the processing of personal data by service providers (Dutch data protection act) or in the context of law enforcement (Law enforcement data act).

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.

This depends on the provider.

The technical and organizational measures have to be in line with the specific security obligations for retained electronic communications data in Article 13.5 of the Dutch Telecommunications Act and the Administrative decree mentioned in the answer to question 21 and 26 (Besluit beveiliging gegevens telecommunicatie).

More particularly, this decree requires providers to have a 'security plan' and details a long list of criteria which this plan has to comply with. A recent study found that only 72% of providers does have such a plan as required. Especially smaller providers are lacking in this regard.

---

[7] See Agentschap Telecom, ‚Eindrapport Nulmeting Wet bewaarplicht telecommunicatiegegevens' [Final report benachmark Data Retention Act], 3 May 2010, available at http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2010/08/17/eindrapport-nulmeting-wet-bewaarplicht-telecommunicatiegegevens/eindrapport-nulmeting-wet-bewaarplicht-telecommunicatiegegevens.pdf.

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

This would again depend on the providers. Dutch law does contain an obligation to ensure data can be deleted as soon as the retention period has elapsed but providers themselves are free to decide how to guarantee to live up to this obligation in practice. A recent report showed that deletion of data has not yet been a high priority for the industry, but this should change after 1 September of 2010, since after that date the first sets of data should be deleted (the law entered into force 1 September 2009, retention period is one year.).

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

The compliance with notification obligations on government agencies has been the subject of much debate as in practice no such notification tends to take place. The data retention obligations and their implementation do not change this.

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

Not applicable to the Dutch situation.

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)?**

At the level of providers it depends on the provider and probably its size. Large electronic communications providers like KPN have special staff to handle security oversight, whereas smaller providers in the Internet context may not have in-house security auditors.

At the general level, the responsible government agency (Agentschap Telecom) provides for oversight and recently conducted a rather critical study about the state of affairs in the context of ISPs, addressing security and confidentiality concerns. This shows that a proper implementation of the law has some priority.

The Data Protection Authority is allowed to do audits but has not yet done so.

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?**

The standards seem to be derived mostly from industry (such as ISO) standards for electronic communications processing equipment. There are no de iure technical standards in the decree regulating the security of electronic communications data.

(See also the answer to question 21 for more details on the telecommunications data security decree.)

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.

There is no change in this co-operation as a result of the data retention law. The co-operation is formally shaped by law enforcement and national security agency legal powers. For non-historic subscriber data a central clearinghouse is in place that centrally stores and provides access to subscriber data (CIOT) Access to other electronic communications data is communicated directly with providers.

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 request are dealt with on the basis of the rules and treaties regarding the mutual assistance in criminal matters. Those rules are laid down in Title X of the Wetboek van Strafvordering [Code of Criminal Procedural Law]. All requests have to be sent to the public attorney's office. No judicial involvement is required in the context of subscriber, traffic or location data.

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).

Data retention and access to electronic communications data has been one of the central issues in the Dutch debate about growing surveillance measures in the information society over the last decade. Other prominent issues have been the closely related issue of access to electronic communications data and the also related issue of wiretapping.

The Dutch parliament and in particular the Dutch Senate (the second and politically secondary chamber in the Dutch parliamentary system) has been highly critical of and resistant to plans for data retention obligations since they were introduced at the European level through a Framework Decision proposal in 2004/2005. No data retention obligations (other than specific obligations related to pre-paid mobile

telephony) existed at that time in Dutch Telecommunications Law. At the time of that EU Council proposal the Dutch parliament demanded from the Minister of Justice (Donner) that he would prevent such a proposal from being agreed upon at the EU level. As regard the later European Commission proposal (first pillar) the Dutch parliament asked the minister to do the same. After the European Council and Parliament came to their compromise in the end of 2005 and the directive was officially adopted in 2006 the Minister of Justice defended this outcome against a majority of Dutch parliament by stressing that he had made it possible to choose for minimal data retention periods (6 months).

Inside the Dutch political system, left, left-leaning and progressive liberal parties were most strongly opposed against data retention obligations. This is in line with opposition against similar surveillance measures. However, in the case of data retention in the Netherlands and in comparison with other issues such as wiretapping laws, opposition was more spread across the political spectrum. Conservative Liberals (VVD) and Christian Democrats (CDA) were also critical of data retention, especially in the Senate. The Conservative Liberals (VVD) placed more (than other parties) emphasis on the possible negative impact on the industry and competition, whereas the Christian Democrats (CDA) in the Senate were highly critical of the proposal on the basis of the whole range of arguments against data retention, including its proportionality, its rationality, and its impact on society and industry. This opposition by the Christian Democrats in the Dutch Senate (against a government coalition in which CDA participated and against a minister of Justice of the CDA) was strongly shaped by Dutch CDA Senator Hans Franken, also a professor of ICT law at Leiden University. This could be seen as an example of how Dutch Senators are less strongly disciplined by their political parties as their party members in the primary chamber.

After a draft proposal to implement data retention had been made public in the end of 2005, the debate polarized more along traditional political lines. The draft proposal was well received by law enforcement related entities and conservative political parties in the Dutch primary chamber of parliament. It was highly critically received by the left, left-leaning and progressive liberal parties, as well as the Dutch data protection authority, which delivered a strongly critical opinion in the beginning of 2006.[8] Conservative parties advocated for the maximum possible retention periods and others advocated for minimal implementation. At no point the option not to implement the Directive at all was seriously discussed.

After the primary chamber of parliament adopted the proposal lowering the proposed retention period from 18 months to 12 months to address privacy interference proportionality concerns, the Senate took a long time to debate the proposal and ended up making a compromise with the Dutch government. This compromise was again strongly influenced by CDA-Senator Hans Franken who announced his decision as choice for ‘political reality over scientific rationality’. Senator Franken remained strongly critical of data retention and proposed a number

8 See Dutch DPA 2007.

of parliamentary motions to address concerns in upcoming evaluations of data retention laws at the Dutch and European level.

Civil Society in the Netherlands was also actively campaigning against data retention since the proposals at the European level. Dutch digital rights organization Bits of Freedom was particularly active with their campaigns at the Dutch and EU parliamentary level. Other groups that opposed data retention were for instance the Dutch consumer organization (consumentenbond). From the industry side, public interest oriented Internet Service Provider XS4all was most active in the campaign against data retention obligations. Other opposition was offered by academics, who repeatedly expressed concerns over the far stretching character of data retention from the perspective of fundamental rights.[9]

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)?

There are such obligation arising from tax law and obligations arising from employment and social security law.

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.

An important study of effectiveness of data retention that played an important role in the Dutch political debate was carried out by Erasums University and published in 2005. The study is titled 'Whoever keeps something has something. Investigation into the use of and need for a retention duty for historical traffic data from telecommunication traffic' and addressed the usefulness and necessity of data retention for historic electronic communications traffic data.[10] The study's conclusion, that a data retention obligation for historic electronic communications data should be introduced with a period of 12 months has been criticized by civil society, industry and the Dutch Data Protecton authority.

As regards internet related data evidence used was anecdotal (a number of interviews with law enforcement officials at the closing of the study). As regards telephony, the core of the study, the researchers based their findings on empirical

---

9 See Bert-Jaap Koops, Egbert Dommering, Nico van Eijk, Paul de Hert, Aernout Schmidt, Jan Smits, Bart Jacobs, Sandro Etalle, Pieter Hartel, Henk van Tilborg, Ybo Buruma, Paul Mevis, Theo de Roos, Taru Spronken, Piet Hein van Kempen, 'Vrijwillig op weg naar de politiestaat' [On a voluntary road to the police state], 2 april 2008, http://www.nrc.nl/opinie/article1873883.ece/Vrijwillig_op_weg_naar_de_politiestaat.

10 'Wie wat bewaart die heeft wat. Een onderzoek naar nut en noodzaak van een bewaarverplichting voor historische verkeersgegevens [Whoever keeps something has something. Investigation into the use of and need for a retention duty for historical traffic data from telecommunication traffic], Erasmus University Rotterdam, June 2005, available at http://www.eerstekamer.nl/eu/behandeling/20050616/rapport_bijlage_bij_brief_5357934/f=/vh1iiavsmqwi.pdf.

data and interviews with the law enforcement sector, but the data in the report itself seemed to show that in most cases data, as wanted by law enforcement agencies, had been readily available.

In its advice of 22 January 2007 on the government's proposal to implement the Directive, the Dutch DPA discussed the report's conclusion on the adequate period for retention of electronic communications data as follows, quoting the Erasmus study:

> "The researchers obtained 65 investigation files, in which traffic data from fixed and mobile telephones played a significant part. They established that the traffic data were available from the providers in virtually all cases. "The data asked for by the investigation agencies were supplied in virtually all of the investigated cases."
>
> The selection did not contain any files where Internet traffic data played a part. The researchers went on to hold discussions with police and the Ministry of Justice on the desirability of a longer retention period. "Since no valid conclusions could be drawn on the basis of the file investigation in relation to the use and need for a retention period (or an extension thereof), it was decided to obtain a greater insight into the problems experienced by law enforcement agencies in relation to obtaining historical traffic data concerning communication via Internet service providers, by means of interviews and a round table discussion."
>
> It was on the basis of these discussions, and not on the basis of the investigation into actual use of traffic data, that the conclusion was reached that a retention period of one year would be desirable for all traffic data. This already incorporates a significant margin in relation to the cases investigated in practice."[11]

Even though the conclusions of the report were debatable, as is clear from the discussion offered by the Dutch Data Protection Authority cited above, an analysis of the legislative history of the Dutch data retention act shows that this conclusion played some role in shaping the compromise for a retention period of exactly 12 months as there was no other independent research concluding otherwise and political parties were polarised between a maximum and minimum retention period. The Dutch government used the conclusion in the study to argue that 12 months should be considered a minimum of what is necessary for law enforcement purposes and proposed an 18 month term. Some political parties argues for a minimal period of 6 months. The 12 month period ended up as a compromise.

---

[11] Dutch DPA 2007.

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

No, no such data on the impact on communications habits in Dutch society are available.

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

Yes, there have been some discussion in parliament during the discussions about the data retention act about either extending or restricting data retention laws.

First of all, the Dutch Senate made a compromise that the retention period for internet traffic would be lowered to 6 months but this promise has not been lived up to by the Dutch Government. The Dutch primary political chamber of parliament also seems opposed to such a change.

In particular with regard to internet data, modification of the data retention obligation has been discussed. The Dutch Minister of Justice has implicitly argued to extend data retention to a range of new online communications services, as it would be ineffective otherwise. The ineffectiveness could also be seen as a reason to retract the opbligation or further restrict it. The Dutch Senate was not convinced of the effectiveness of retaining internet traffic data and concluded on this basis that the necessity of a data retention obligation was insufficiently evident. As part of the compromise in the Senate to pass the implementation bill, the Dutch Minister of Justice has informed the European Commission of the Dutch Senate's concerns in its letter of 1 July 2010.[12]

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

---

[12] Dutch Minister of Justice, letter to Commissioner Cecilia Malmström regarding the evaluation of Directive 2006/24/EC, 1 July 2010, http://www.eerstekamer.nl/behandeling/20100701/brief_van_de_minister_van_justitie/f=/vigjigs1bhix.pdf

fundamental rights. As regards the right to secrecy of telecommunications: Which data are – according to national (constitutional) law[13] – considered as telecommunications content? Is it legal under national (constitutional) law to retain this content without a *specific* reason?

Fundamental rights are protected in Dutch law in the Dutch Constitution and through the direct effect of fundamental rights in international treaties in the Dutch legal system. In particular the European Convention of Human Rights (ECHR) has a direct and strong impact on fundamental rights protection in the Dutch legal system.

The Dutch legal system has a weak constitutional challenge tradition and no constitutional court. The Dutch constitution provides that parliamentary legislative acts cannot be constitutionally challenged in Court (lower rulemaking can be challenged). However, it also provides that laws have to be in accordance with valid international law, which includes the ECHR, and can be challenged on the basis of provisions in such international law which have so-called direct effect. Most provisions in the ECHR have such direct effect. In addition, law could be challenged on the basis of European Union law, which also provides for fundamental rights protection. To conclude, the most important protection of fundamental rights in the Dutch legal system is provided for by the ECHR.

Dutch Constitution (Grondwet, Gw)

General protection of private life is provided for in Article 10(1) Gw. Restrictions are possible by or on the basis of primary legislative acts.

Protection of informational privacy in Article 10(2) Gw. There should be laws that protect the right to private life in the context of the registration and provision of personal data.

Right to access to personal data in Article 10(3) Gw. The law has to make rules about the possibility to gain knowledge about one's registered personal data and the use thereof, as well as the correction of such data.

Confidentiality of communications is provided for in Article 13 Gw. The first paragraph provides that the confidentiality of postal correspondence is inviolable. The second paragraph provides that confidentiality of telephony and telegraphy is inviolable except in the cases provided for by primary legislation by those that have been assigned by or on the basis of such laws. There has been a lot of debate to modernise this article but attempts to do so have been unsuccessful. The result is that new modes of communications are arguably weakly protected under the Dutch constitution, whereas older modes of communication, in particular postal communication, are strongly protected. This means that Art 8 ECHR, which is not as technology dependent plays an important role as regards confidentiality of communications. See Steenbruggen, Publieke dimensies van Communicatie, 2009.

[13] 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).

Freedom of expression is protected in Article 7 Gw, with an emphasis on whether certain rules can be imposed with regard to what media and a ban on prior restraints on the basis of content. Article 7 (1) bans censorship (absolute) of the press. Article 7(2) provides that the law shall regulate radio and television and no prior restraint on content shall be imposed. Since Article 7 Gw is highly specific, article 10 ECHR also plays a major part in freedom of expression doctrine in the Netherlands.

Since the Dutch data retention act is a primary legislative act, it is impossible to invoke any of the rights mentioned above against the constitutionality of the act. Parliament is entrusted with the enforcement of the constitution as regards its legislative acts. Usually the Senate is considered as the constitutional conscience of the system. The fact that the Senate agreed to pass the act, even though there were still strong constitutional concerns across the political board, shows the relative weakness of this guarantee.

The official legal debate about the proportionality of data retention from the perspective of fundamental rights has almost completely been dealt with through the lens of Article 8 ECHR, the protection of private life. The major concern addressed was typically whether data retention was necessary in a democratic society, considering the revealing nature of the electronic communications data for one's private life. Concerns from the perspective of freedom of expression and information have not really entered the Dutch debate. Concerns about the confidentiality of communications have been addressed but not as prominently; the argument being that traffic and subscriber data could actually reveal much about the content of communications.

The division of content and traffic data is based on the same distinction as made in European telecommunications law.

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?

Under the conditions outlined above for each respective right. In short, the only real condition is that restrictions be prescribed by primary legislative acts. The substantive conditions of Article 8 ECHR play a more important role, in particular the restriction that interferences be necessary in a democratic society.

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, there is no such ruling. The ruling of the German Constitutional Court has had a impact on the political and legal debate but not changed that debate. The political interpretation of the ruling was superficial.

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?

No, it does not provide such a 'collective' freedom of surveillance threshold or limit.

Balancing takes place in individual cases in which other surveillance measures could play a role if they are relevant.

Usually, the Dutch parliament, which is responsible for ensuring primary Dutch legislation is in accordance with constitutional rights, does not consider public surveillance measures collectively, although sometimes an assessment or reference to other (related) surveillance measures can play a role in the political debates about the legitimacy of proposed new interferences.

A good example in the context of the transposition of the data retention directive was the fact that Dutch Criminal Procedural Law already contained quite far reaching powers to gain access to these data, such as the power to request complete files or part of files (Art 126hh, discussed above). The government argued that this was a separate legal matter. The data retention law only related to availability, while access to data was already covered by existing laws. Some members of parliament argued, unsuccessfully, that the amount of data that would be available, implied those existing powers would interfere more severely with fundamental rights and should therefore be restricted.

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 it does not require such exemptions to be made. If the ECHR or ECJ would come to the conclusion that fundamental rights do require such exemptions to be made, Dutch law, in the broad sense, would directly require the same.

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 Dutch Constitution does not protect professional freedom as such. Dutch law does contain a general legal principle that a certain class of private actors cannot be obligated to pay for a legal regime that is actually for the general public good. Professional freedom would be derived from European law market freedoms or CoE international law. There has been a challenge to the limited reimbursement of wiretapping costs under Dutch law which have (unsuccessfully) raised European

market freedoms and the general principle mentioned above. The principle is valid but primary legislative acts cannot be annulled in Court due to the Dutch Constitution. Ultimately, the Court did not have to reach a conclusion on the validity of the claim based on an analysis of a possible breach of the substantive constitutional norm. The case has not proceeded to the Court of Appeals.

More generally, over the last decade, there has been a fundamental legal debate in the Netherlands about the requirements on professional private entities and unrelated public agencies to systematically assist law enforcement agencies.[14] At the core of the debate was the question how far law enforcement agencies could go in asking private and public entities at large for information about private persons. In practice, the telecommunications sector, the financial sector and also the travel sectors have been increasingly and systematically targeted as a source of information for law enforcement. Dutch law has followed this tendency by imposing specific legal powers to request for information from these sectors, first by introducing specific legal powers to request for information in the telecommunications and financial sector (2002-2005). Since 2006, there is a general law that allows law enforcement agencies to demand (personal) information from any private or public entity if its relevant to an investigation. Notably, the debate about these laws addressed fundamental rights concerns from the perspective of the data subjects, not from the perspective of fundamental rights to professional freedom.

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)?

See the answer to question 11.

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

Investment costs are not reimbursed and there are standard tariffs in legislation for reimbursement of obligated parties.

The lack of full reimbursement has been the subject of ongoing debate and litigation, XS4all against the Dutch state. Rb 's-Gravenhage 21-2-2007, 239632 / HA ZA 05-1009III. The basis for the challenge of the lack of full reimbursement was European law (EU market freedoms and CoE fundamental protection of

[14] See (ALL IN DUTCH) e.g. Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, Gegevensvergaring in strafvordering, Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek, Den Haag, 2001; E.C. Mac Gillavry, 'De voorstellen van de Commissie-Mevis - dwangmiddelen voor de informatiemaatschappij', NJB (76) 2001-30, p. 1411-1418. P.A.M. Mevis, 'Gegevensvergaring in de informatiemaatschappij: een strafvorderlijke informatieplicht?, II Gegevensvergaring is iets anders dan een informatieplicht.', RM Themis 2002-1, p. 30-35; E.C. Mac Gillavry, Met wil en dank, Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, proefschrift,Wolf Legal Publishers 2004. L. Stevens, B.J. Koops & P. Wiemans, `Een strafvorderlijke gegevensvergaring nieuwe stijl´, NJb (79) 2004-32, p. 1680-1686.

property) and the general principle that specific private parties cannot be required to pay for general measures for the public good that are not directly related to their activities. The Court however ruled that the Dutch constitution made such a challenge to a legal rule provided for in primary legislation impossible and the appeal has been retracted by the telecommunications provider.

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 Dutch Constitution provides that Dutch laws (including primary legislative acts) have to be in accordance with valid international law, which includes the ECHR, and can be challenged on the basis of provisions in such international law that have so-called direct effect (artt. 93 and 94 of the Dutch Constitution). Provisions have direct effect if they have the substantive character that they can be generally binding.

Does this mean that international treaties rank below the Constitution, but above other national law in the hierarchy of norms?

In the Dutch legal order, international treaty law ranks higher than the Dutch Constitution, which in turn ranks higher than national law and legislaton. International treaties that are not in line with the Dutch Constitution can only be ratified after an amendment of the Dutch Constitution.

Dutch primary legislation can not be challenged on the basis of the Dutch Constitution but it can be challenged on the basis of provisions with direct effect in international treaties, such as Article 8 and 10 ECHR.

Most provisions in the ECHR, and in particular Art. 8 and 10 ECHR, have direct effect. In addition, law could be challenged on the basis of European Union law, which also provides for fundamental rights protection. To conclude, the most important protection of fundamental rights in the Dutch legal system is provided for by the ECHR as interpreted by the Dutch courts.

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?

Directives are typically transposed by separate legal acts, which either make a new law or amend existing law. The procedure is similar as for any other primary legislative act.

1.Government prepares act

2. Asks advice to the Council of State

3. Send proposal including advice plus a government reaction to the Parliament

4. Parliament's primary Chamber (Tweede Kamer) prepares legislative report with questions, etc., debates act in commission and plenary session, proposes possible amendments and votes on acts and amendments.

5. Parliaments secondary Chamber (Eerste Kamer) prepares legislative report with questions, etc., debates act in commission and plenary session, and votes on act. Can not make amendments

6. Act is published and signed into law.

Directives which are not transposed or not correctly transposed have direct and or indirect effect on the Dutch legal order in accordance with the case law of the ECJ. In addition, certain provisions in EU law could have direct effect on the basis of the Dutch Constitution.

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?

International treaties that are not in accordance with the Dutch constitution can only be ratified by the Dutch parliament through a similar procedure as is needed to amend the Dutch Constitution.

The Dutch Constitution requires that the Dutch government advance the international legal order (Art 90) and makes it possible to challenge Dutch law on the basis of valid international law (art. 93 and 94). The Dutch legal system does not traditionally allow for the kind of challenges that work the other way around.

Fundamental rights protection under the Dutch constitution does not provide much extra in terms of protection in comparison with European law or the European Convention.

Possibly, in the field of the press, the Dutch constitution provides for very strong protection against prior restraints, but since this is a field in which the EU has no clear mandate to regulate in way that would go further than the Dutch constitution allows, this is unlikely to be an issue.

The Dutch Constitution does not contain a provision which specifically limits the possibility to confer sovereign rights to the EU. European Union or other international treaties that are not in line with the Dutch Constitution can only be ratified after an amendment of the Dutch Constitution.

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 division of power follows the decentralized model of data retention at the provider level. They are responsible for acting in accordance with the law (to retain data, to secure them and provide access when legally demanded, and to delete after period is elapsed).

Law enforcement and national security has official legal powers to demand access to data. The Agentschap Telecom oversees the proper implementation of the law and its execution. There is no regional division of powers.

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

There are such limits on the basis of the EU general privacy directive (95/46/EC) on the possibility to process data outside of the EU in countries without appropriate data protection laws, but no specific limits on the transfer of retained electronic communications data within the EU have been set in the context of data retention law.

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?

There are a number of options that in my opinion could improve the balance of the interests of effective tools for law enforcement and national security interests and the interests of communications freedom in the information society in the Netherlands.

Currently, the retention period of 12 months in the Netherlands is relatively arbitrary and more than provably necessary on the grounds of available data and research. As a result, the data retention period should be limited (considering the requirements of Article 8(2) ECHR). Until sufficient proof is given, it would be better to lower the retention period to 6 months or to abolish data retention altogether. This decision should be made in view of a careful debate about the possibility to improve retention of electronic communications data in specific cases (e.g. freezing orders).

The Dutch debate about data retention has rightfully considered the impact of data retention on the fundamental right to private life but has mostly ignored the possible impact on other fundamental freedom such a s the right to freedom of expression. There is a lack of understanding of the fundamental instrumental character of privacy in communications for other fundamental rights. The lack of exceptions for

certain categories of subscribers can be explained by this lack of understanding of data retention on other fundamental interests. A better understanding would probably lead the Dutch legislature to adopt such exceptions.

More generally, a majority of Dutch politics has failed to adequately qualify the impact of communications traffic and location data if retained for long periods of time to be available for law enforcement and national security purposes if they arise. Time and again, the government could make the argument that the only real impact on people's privacy would be made if data were actually accessed by those agencies, reducing the concerns about blanket data retention to mere concerns about confidentiality and secrecy.

In line with the above, it would be an improvement if retained data were only available in cases of really serious crime, meaning that a list of really serious crime would be actually provided for in the law.

Access to one's own electronic communications data should be improved and better enforced as well as the requirement of notification when data have been accessed.

Another problem is that the data retention act's impact on fundamental freedoms can only be rightly assessed if the new rules are seen in the general context of existing laws and obligations that govern electronic communications data's registration, availability and accessibility to actors across Dutch society. The data retention act, however, only transposed the retention obligations. A range of other rules, such as the powers to access data and perform data-mining on them, now have a significantly stronger impact.

From an academic perspective, there is a need to do more Netherlands specific independent studies as to the effects of data retention on law enforcement's effectiveness, on Dutch society and on the electronic communications landscape.

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

The Netherlands

Mr. Drs. J.V.J. van Hoboken

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, Dutch constitutional law does not provide for a specific right to communicate anonymously. In a recent legal dissertation about the legal protection of anonymous communication, Anton Ekker concluded that there are several dispersed elements in Dutch telecommunications and media law that show the contours of a right to communicate anonymously.[1] However, Dutch law does not provide for a specific right to communicate anonymously. An exception, resulting from several judgments of the ECtHR involving the Dutch State, is the protection of journalistic sources (See e.g. ECtHR 22 November 2007 (Voskuil)). The Dutch Legislature is planning to codify this case law directly into Dutch law.

[1] Ekker, *Anoniem Communiceren. Van Drukpers tot Weblog,* Anton Ekker, 2006.

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

There is still wide support to lower the retention term for retained internet data to the minimum of 6 months. Currently, the term is still 12 months. The Dutch government promised the Senate, when it passed the data retention implementation act, to follow up with such an amendment of the law. However, as explained in the previous questionnaire, the primary chamber in the Dutch Parliament is not clearly in favour of lowering the term for internet data.

Another possible amendment that is currently being discussed and which may have considerable political support, is the cost reimbursement for small providers on which data retention obligations weighs relatively more heavily. The lowering of the retention term can also be seen as a means to lower the costs of data retention obligation for Internet Service Providers.

Besides these relatively minor elements of possible modification and improvement of the current implementation at the national level, most attention in the polical debate about data retention goes out to the evaluation at the European level and to a lesser extent to the various rulings about the constitutionality of data retention in other member states. The Dutch Senate, when passing the data retention law in July 2009, adopted a motion that requested the Minister of Justice to provide all the necessary input to make this evaluation of the Directive by the Commission as meaningful as possible and to notify the European Commission of the specific concerns of the Dutch Senate about the effectiveness of the retention of internet data.[3] On 8 February 2011, the relevant Dutch Senate Commission sent a critical letter to the Minister of Justice about its input for the evaluation. In particular, it considered the input not in line with the adopted motion in 2009 and the promise by the government to act in line with this motion.

Apart from telecommunications and internet providers, systematic resistance to data retention and proposals for amendment has come from Dutch civil society

---

[2] E.g. plans to halve the storage period from one year to six months currently seem to gain momentum; see: http://www.telecompaper.com/news/data-retention-corrective-law-goes-back-on-dutch-agenda. Could you provide some more information on these – and other relevant – developments (see also your answer to question 49 of the first questionnaire)?

[3] Gewijzigde motie-Franken (CDA) c.s. over de effectiviteit van de opslag van gegevens (EK 31.145, N), http://www.eerstekamer.nl/motie/gewijzigde_motie_franken_cda_c_s/document/f=/vi6mbd6hishc.pdf.

organization Bits of Freedom. Bits of Freedom has been actively campaigning against data retention since 2004. Recently, Bits of Freedom has been active at the national and European level in the evaluation of the Directive and is one of the authors of the civil society shadow report of European Digital Rights, responding to the official EC evaluation.[4] Bits of Freedom's reports and press releases about the developments relating to data retention, which carry most of the arguments made in this shadow report, manage to get quite some media attention. In particular, the Quick freeze option is proposed in this context. Still, a structural revision or amendment of data retention is not a widely debated issue in the Netherlands and Dutch politicians seem to await the results of the evaluation at the European level.

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?

Dutch penal law contains several standard provisions with regard to the reactive obligation to cooperate for private parties with law enforcement agencies such as the obligation to hand over physical goods (art 96a and 105 Dutch Code of Criminal Procedure) or the obligation to testify in front of a judge (art. 210 Dutch Code of Criminal Procedure).

As described in the previous questionnaire (question 55), over the last decade, there has been a fundamental legal debate in the Netherlands about the requirements on professional private entities and unrelated public agencies to systematically assist law enforcement agencies.[5] At the core of this debate was the question how far law enforcement agencies could go in asking private and public entities at large for information about private persons. In practice, the telecommunications sector, the financial sector and the travel sectors have been increasingly targeted as a source of information for law enforcement and national security agencies. Dutch law has followed this tendency by imposing specific legal powers to request for information from these sectors, first by introducing specific legal powers to request for information in the telecommunications and financial sector (2002-2005). As the final outcome, since 2006, there is a general law that allows law enforcement agencies to demand (personal) information from any private or public entity (not

---

4 European Digital Rights, Shadow evaluation report on the Data Retention Directive (2006/24/EC), 17 April 2011, http://www.edri.org/files/shadow_drd_report_110417.pdf

5 See (ALL IN DUTCH) e.g. Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, Gegevensvergaring in strafvordering, Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek, Den Haag, 2001; E.C. Mac Gillavry, 'De voorstellen van de Commissie-Mevis - dwangmiddelen voor de informatiemaatschappij', NJB (76) 2001-30, p. 1411-1418. P.A.M. Mevis, 'Gegevensvergaring in de informatiemaatschappij: een strafvorderlijke informatieplicht?, II Gegevensvergaring is iets anders dan een informatieplicht.', RM Themis 2002-1, p. 30-35; E.C. Mac Gillavry, Met wil en dank, Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven, proefschrift,Wolf Legal Publishers 2004. L. Stevens, B.J. Koops & P. Wiemans, `Een strafvorderlijke gegevensvergaring nieuwe stijl´, NJb (79) 2004-32, p. 1680-1686.

acting in a personal capacity) if it is relevant to an investigation. The law also contains a legal power to order the cooperation of private parties with regard to the recording of future data (for maximum 3 months), a legal power which is comparable to a general quick freeze.

These obligations are all reactive in nature. There are some obligations, in the financial and electronic communications sector in particular, that require pro-active cooperation. There is a obligation on hotels to register visitors (Art 438 Dutch Code of Criminal law). In the financial sector, there is a general obligation to be able to identify customers and there are some more recent obligations resulting from the implementation of the Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

In the electronic communications sector, besides data retention, there are obligations on public electronic communications providers and networks to be able to wiretap their systems.

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?**

Article 218 of the Dutch Code of Criminal Procedure provides for specific exemptions to the obligations to testify or deliver evidence for two categories of people, close relatives on the one hand and those that are obligated to keep confidentiality due to their profession on the other hand. These professionals are traditionally lawyers, notaries, doctors and clericals. Bankers, electronic communications providers and accountants are not covered. Journalists are protected as a result of case law of the ECtHR about Article 10 ECHR and the protection of journalistic sources (see also question 1).

The Dutch implementation of the data retention directive does not provide for an exception with regard to the data of these professionals. The legal powers to gain access to the data contains an exception that bans requests of data from people that can claim protection under article 218 *themselves*. This means, in theory, that a telephone company's employee could refuse to cooperate if the request relate to telephone traffic of a close relative.

The situation is similar in the case of wiretapping powers, which is most relevant with regard to lawyers. The specific wiretapping powers in Dutch law do not provide for a codified exception if the subject of the wiretapping order to a telecommunications company is (known to be) a lawyer. However, this does not mean these powers can be used without taking account of the professional duties to keep secrets of lawyers (or others that can claim protection under Article 218 Dutch

Penal Code). In fact, it is standard jurisprudence that these powers cannot be used with regard to lawyers and other professionals protected by art. 218, if they are targeted when acting in their professional capacity.[6] There is an obligation on the public prosecutor's office to destroy evidence that is obtained through the use of investigative powers that a protected professional could refuse to testify about on the basis of Article 218 (Article 126aa Code of Criminal Procedure).

Whether the absence of a restriction on data retention of protected professionals is legally problematic – the Dutch government has simply argued that the mere retention of data related to protected professionals is not a problem under Article 218 and only the actual access to those data could constitute a problem - is an open legal question which is unaddressed by the data retention implementation law and the current literature on the subject. Even if this absence of restrictions on data retention is permissible, it can be argued that the legal powers to request access to telecommunications data may be similarly restricted (as in the case of wiretapping) if the data subject is (known) to be a protected professional and if they are targeted when acting in their professional capacity.

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

The data will be stored and processed by the requesting public (law enforcement) authorities. They have to adhere to the rules in the Law Enforcement Data Act. Most specifically, Article 4, paragraph 3 of this act provides that the respective agents ensure that

- data are correct and precise and incorrect or incomplete data are corrected, completed or deleted.
- data are deleted when the storage is no longer necessary for the purpose they were processed for or when a legal obligation requires their deletion.
- appropriate technical and organizational measures, taking into account the current technical possibilities and the costs of operations on the one hand and the risks attached to the processing of police data on the other hand, are made to ensure an appropriate level of data security.

With respect to the appropriate level protection, recently, the Dutch Data Protection Authority has clarified that data security can be considered appropriate if it is in line with the NEN norm: NEN-ISO/IEC 27002:2007.[7]

---

6 Dutch Supreme Court (Hoge Raad) 10 April 1979, NJ 1979, 374; Dutch Supreme Court (Hoge Raad) 17 May 1988, NJ 1989, 439.

7 College Bescherming Persoonsgegevens, Onderzoek CIOT-Bevragingen, Onderzoek Dienst Nationale Recherche, April 2011, http://www.cbpweb.nl/downloads_pb/pb_20110428_ciot_db_dnr.pdf.

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

In its response to the EC evaluation in the end of 2010, the Dutch government provided some statistical estimates. The response has been made public as a result of a freedom of information request by a Dutch activist.[8]

In its response, the Dutch government writes that it estimates (without further clarification) that in 65% of all law enforcement investigations use is made of historic electronic communications data. The government estimates that in 2010, a total of 85.000 requests for historic electronic communications data will have been made, an increase of 9% in comparison to the estimates about 2009. In comparison, a total of circa 3 million requests for current subscriber data are made each year by law enforcement agencies through the CIOT (central storage of current subscriber data).

B. Questions to the experts from only some of the Member States

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

As explained in detail in the first questionnaire, the Dutch legal system has a weak constitutional challenge tradition and no constitutional court. The Dutch constitution provides that parliamentary legislative acts cannot be constitutionally challenged in Court (lower rulemaking can be challenged). However, it also provides that laws have to be in accordance with valid international law, which includes the ECHR, and can be challenged on the basis of provisions in such international law which have so-called direct effect. Most provisions in the ECHR, including Article 8 and 10, have such direct effect. In addition, law could be challenged on the basis of European Union law, which also provides for fundamental rights protection. To conclude, the most important protection of fundamental rights in the Dutch legal system is provided for by the ECHR As a result, the constitutionality of the Dutch implementation law can only be tested in the broader European legal context.

It is my opinion that the current data retention law in the Netherlands highly problematic for 3 main reasons relating to the fundamental protection of private life, confidentiality of correspondence and the right to freedom of expression and information. These reasons are the following:

---

8 Answers Dutch Govermment to EC Questionnaire/Evaluation, avaliable at https://rejo.zenger.nl/files/20100902-brief-minjus-aan-ec.pdf

I. Lack of demonstrated necessity:

The evidence for blanket data retention has consistently been and remains thin. An initial report in 2005 by the Erasmus University in fact showed that historic data for wireline telecommunications were available in almost all cases; hence no retention obligation would have been necessary. In their pleas for long term blanket data retention, proponents have mostly used undocumented estimates and arguments that do not make a fair comparison to a situation in which data retention would not exist or alternatives such as a quick freeze would be chosen instead. In addition, the alternatives for voice communications that exist in the networked information environment make the current scope of data retention obligations with regard to traditional and mobile voice communications or specific internet communications protocols questionable. All in all, the evidence of the actual necessity of blanket data retention of electronic communications data is very thin.

II. Nature of the obligation

The interference of the obligation to retain all electronic communications data for lengthy periods of time for law enforcement purposes with the fundamental rights of Dutch citizens is significant by nature. The active and systematic use of electronic communications networks has become a prerequisite for effective participation in the information society. The free use of these networks as called for by the right to freedom of expression and information, the right to confidentiality of communications and the right to private life more generally is placed on its head by the introduction of blanket data retention. To place the entire communicative activities of populations under systematic surveillance because the data may be later useful for the prevention or prosecution of crime, including crimes unrelated to the use of electronic communications networks, is highly problematic considering the constitutional values underlying open democratic societies.

III. No restrictions (for instance on access) where possible or necessary.

As the ECJ decided, the directive itself does not address the question of access to retained data. At the same time it is clear that the interference of blanket data retention with the fundamental rights of citizens can only be justified taking account of the actual use of the data. In other words, the constitutionality of data retention cannot be adequately assessed without taking into account the legal powers to gain access to retained data and the actual use of those powers by public authorities.

This also means that the European legislator has shifted the burden to the Member States to establish the right balance between data retention and the access and use of those data on the one hand and the fundamental rights of citizens on the other hand. In the Netherlands, however, the legislator has refused to consider the new data retention obligations in light of the already existing powers to gain access to data. In addition, it has argued that a blanket

data retention obligation is not a heavy interference with the rights of citizens because it would merely require service providers to keep data, whereas only when data are accessed a real interference would take place. The result of this line of reasoning has been that the directive's implementation has not led to a proper evaluation of the impact of data retention in practice (retention, access and use). Another result is that the Dutch legislator has not carefully studied the ways in which proper restrictions, in view of the fundamental rights of citizens, could have been made. Examples of such restrictions are the possible restriction on retention of data of certain professionals (see answer to question 4) or maybe even more importantly the restrictions in terms of the crimes investigated that would allow for the use of retained data. The absence of similar restrictions in Dutch law make it even harder to argue that the Dutch implementation of the data retention directive is carefully crafted in view of the necessary justification of its interference with the fundamental rights of Dutch citizens.

8. **Are the data to be retained in accordance with the Directive covered by the confidentiality of correspondence, as provided for by the national (constitutional) law of your country (in particular, Art. 13 Gw)?**

   The fundamental rights protection of these data is derived from Article 8 ECHR. Article 13 of the Dutch Constitution only protects the content of communications.

   Of course, the retained data do fall under the protection provided for by the ePrivacy directive and its implementation into Dutch telecommunications law (Chapter 11).

9. **In your answer to question 59 of the first questionnaire, you state: "Directives which are not transposed or not correctly transposed have direct and or indirect effect on the Dutch legal order in accordance with the case law of the ECJ. In addition, certain provisions in EU law could have direct effect on the basis of the Dutch Constitution." Could you please provide details under which conditions EU law may have direct effect on the basis of the Dutch Constitution? Which constitutional provisions apply in these cases?**

   The Dutch Constitution provides that Dutch laws (including primary legislative acts) have to be in accordance with valid international law, which includes the ECHR and the body of EU law, and can be challenged on the basis of provisions in such international and European law that have so-called direct effect (artt. 93 and 94 of the Dutch Constitution).

   More specifically, Article 93 and 94 of the Dutch Constitution provide for the direct effect and prevalence in Dutch law of provisions in international treaties or in decisions of international public organizations that have the character that they may be binding on all persons.

Article 93

Provisions of treaties and of resolutions by international institutions, which may be binding on all persons by virtue of their contents shall become binding after they have been published.

Article 94

Statutory regulations in force within the Kingdom shall not be applicable if such application is in conflict with provisions of treaties that are binding on all persons or of resolutions by international institutions.

These 2 provisions are particularly important in relation to the ECHR. For EU law, the ECJ has established its own European-wide doctrine on direct and indirect effect of European law, which makes the existence of these provisions in the Dutch constitution less significant in practice.

10. What considerations during the legislative procedure have led to the deviation between the Directive and the national law in terms of the location data to be retained (also during the communication)? Was the legislator aware of the fact that under the Directive only location data generated in the moment of initiating a connection may be retained? If so: was the legislator of the opinion that it is not contrary to EU law to extend the data to be retained beyond what is provided for by the Directive?

The Dutch government, when offering its draft implementation law in the end of 2006, argued that this extension of the retention obligation to location data during calls, was an extension of the obligation to record such data that already existed in Dutch law for mobile pre paid telecommunications (The former Decree Special Collection Subscriber Data (Besluit bijzondere vergaring nummergegevens)). In its reaction to this draft implementation law, the Dutch Data Protection Authority made the government aware of the fact that this former obligation was not a retention obligation but a reactive obligation to analyse existing data sets restricted to the identification of pre paid telephony subscribers. It also clarified that these data had been purposefully excluded from the Directive's scope as a result of a debate in the European Parliament. The official implementation law by the Dutch government still contained the same line of reasoning. The retention of these location data during calls is an extension of the former obligations relating to the identification of pre paid subscribers (Dutch law does not require that pre paid subscribers are identified directly).

Article 15 of Directive 2002/58/EC implies that the introduction of data retention obligation for other data, such as the location data during calls, is (in principal) legally permissible under European law. The Directive's harmonization character as regards the type of data to be retained in the member states is minimal, not maximal or complete.

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

    This rule, which can be found in consideration 13 of the Directive has not been specified into Dutch law.

12. **Regarding the case-law drawing on general tort principles as a legal basis for access to retained data by private litigants (as referred to in your answer to question 15 of the first questionnaire):**

    - **Do litigants have to seek an order by the court competent in the case, requesting these data, or do they dispose of an own right to request the data themselves without such order?**

      They can seek an order by a court but the duty of care on the basis of general tort law implies that service providers are expected to respond to a request voluntarily.

    - **Has the jurisdiction been legally/constitutionally questioned by anybody in the past (courts, individuals party in a court case, media/public opinion)? If so: please provide details on the debate/relevant jurisdiction.**

      Yes, this duty of care to provide identification data to private parties on request has been contested by electronic communications providers in court and led to public debate and coverage in the media.

      The most important legal decision establishing this duty of care has been the decision of the Dutch Supreme Court in Lycos/Pessers in 2005. This case involved a dispute between a private individual (Pessers) over a damaging publication on a website hosted by *hosting provider* Lycos. Pessers demanded the identification data from Lycos to be able to take the actual wrongdoer to court. The Court decided that under certain circumstances – most notably if there is sufficient proof for an alleged unlawful act by the targeted subscriber and there are no alternative means to identify– there is a duty of care on the service provider to provide the data. This case law is relevant from the perspective of data retention law because this same standard has later been applied by some courts to *internet access providers* in the context of requests by rights holder organization about alleged illegal file sharing subscribers.

      Quite recently, the Dutch government has stated that it wants to restrict the possibility of rights holders to gain access to identification data. It wants to provide for the possibility to gain access to such subscriber data only in cases when a judge has established that infringement on a large scale have taken place.

- **Are you aware of any cases where individuals have been granted access to data retained on the basis of these principles?**

  No, not with respect to the data retained as a result of the data retention directive's implementation. Actual practices of major broadband providers how requests are dealt with may differ but, notably, do not exclude the possibility that they hand over historic subscriber data voluntarily. For example, internet access provider XS4all has an extensive list of criteria that all need to be fulfilled before it would consider handing over identification data, but does not exclude it completely.[9]

13. **Apart from the reimbursement of costs for the handling of data requests (as described in your answer to question 28 of the first questionnaire): are costs for the acquisition and installation of storage equipment that is necessary to fulfil the retention obligations reimbursed as well? If so: please describe the applicable rules in detail. In which form and to which extent (completely, certain percentage of the full costs, lump sum, mere depreciation of book-entry items on tax return) are the costs reimbursed? How and by whom (government authority, provider) are the amounts to be reimbursed calculated? How are the specific data retention costs delimited against the costs for the general storage equipment and the general data storage process?**

  No, these costs (*acquisition and installation of storage equipment)* are not reimbursed.

14. **Please provide more details about where and how the data is stored (see your answers to questions 38 and 39 of the first questionnaire):**

  - **Have discussions on the extension of CIOT to historic traffic and location data so far led to any changes in the place of storage of data retained, or are any changes planned in the future in this regard? Would such a central storage of traffic and location data (enabling entitled bodies to obtain direct access to the data) require a new legal basis?**

    No, central storage of the data has not been implemented and due to recent developments showing problems in the CIOT architecture with respect to the legality of requests, has proven less likely to be implemented in the near future. Several recent reports about the practices of subscriber data access through the CIOT show lacks of compliance with the legal rules. The Dutch Data Protection Authority for instance recently conducted an official audit to test the legality of CIOT requests and concluded that the authorisation of specific law enforcement agency personnel to use the CIOT system is not in line with Dutch data protection law.

---

[9] Complaint Procedure XS4all, http://www.xs4all.nl/overxs4all/contact/media/beleidsregels_klachten.pdf

- **As regards the transfer of personal data to third countries: does Dutch data protection law contain provisions applicable to data retention, which correctly transpose Chapter IV of Directive 95/46/EC? Please describe any potential differences.**

  Chapter IV of Directive 95/46/EC has been implemented correctly into Chpater 11 of the Dutch Data Protection Act (Wet bescherming persoonsgegevens). These data protection rules are also applicable to data retained by communication service providers as a result of Dutch data retention obligations.

15. **The 'Besluit beveiliging gegevens telecommunicatie' provides for a series of technical and organisational measures to ensure secure data storage (see your answer to question 14 of the first questionnaire). Are there any specifications regarding data security with respect to the transmission of retained data to the entitled bodies (objectives to be achieved – e.g. "adequate confidentiality" – and/or quality requirements to be fulfilled – e.g. an obligation to encrypt the data before transmitting them to the authorised bodies)? If so: Please provide details.**

    Notably, the decree mentioned here, which imposes obligations on service providers, does not provide for such specific rules or measures when data are transmitted to requesting agencies. Hence, this falls under the general obligation on operators to ensure data security of Article 13.5 of the Dutch Telecommunications Act.

    The Law Enforcement Data Act, which imposes data protection obligations on law enforcement data processing practices, contains a general data security obligation discussed in the answer to question 5 above (Art 4). Recently, the Dutch Data Protection Authority (CBP) conducted an audit at the National Investigative Police Agency (Dienst Nationale Recherche) and concluded that this provision also applies to the transmission of data to telecommunications operators, for instance when requesting traffic data. It concluded that the current practice, i.e. data are openly transmitted by fax over non-secure telephone lines, is not appropriate from the perspective of Art 4.3 of the Law Enforcement Data Act, and thereby unlawful.

    In the recent report of the Dutch Government (Agentschap Telecom) about the status of compliance with Dutch data retention rules and the decree mentioned above ('Besluit beveiliging gegevens telecommunicatie') by ISPs, note was made of the complaint by operators that whereas they were under strict data security rules, law enforcement requests seemed to adhere to much looser data security practices.

16. **Are the technical and organisational measures necessary to implement these legal requirements standardised or specified in any other way, e.g. through guidelines issued by the supervisory authority? If so: Are these specifications binding or not for the bodies concerned? Please describe their content.**

    With regard to Article 4.3 of the Law Enforcement Data Act, measures are not standardized but need to be appropriate, taking into account the current technical possibilities and the costs of operations on the one hand and the risks attached to the

processing of police data on the other hand, are made to ensure an appropriate level of data security. With respect to the appropriate level protection, recently, the Dutch Data Protection Authority has clarified that data security can be considered appropriate if it is in line with the industry norm: NEN-ISO/IEC 27002:2007.[10]

17. Do these measures apply specifically and exclusively to the transmission of data in the context of data retention, or generally to any data processing (in electronic communications)?

There are no rules specifically related to the transmission of data in response to law enforcement requests (see answers above).

18. Please describe the rules for co-operation between the party retaining the data and the party (public authority) accessing them in detail. What steps have to be followed in each case in order for the respective entitled body to obtain access to the requested data?

Historic traffic or location data can be requested on the basis of Article 126n of the Dutch Code of Criminal Procedure by the public prosecutor's office. The following steps have to be made:

1. The respective agent would have to ensure that the conditions for using the legal power have been met, namely that the data are actually needed for the investigation of a serious offense or crime.

2. The public prosecutor then records the request (vordering) in writing (proces verbaal), in which mention is made of

    a. the crime and if known, the name or else an as precise as possible indication of the suspect;

    b. the facts and circumstances from which it is apparent that the conditions for using the legal power are met;

    c. when known, the name or else an as precise as possible indication of the person whose data are requested;

    d. the data that are being requested.

3. The legal request is sent to the service provider (this is typically done by fax).

4. The service provider responds to the legal request (this is typically done by fax) by providing the requested data.

---

[10] College Bescherming Persoonsgegevens, Onderzoek CIOT-Bevragingen, Onderzoek Dienst Nationale Recherche, April 2011, http://www.cbpweb.nl/downloads_pb/pb_20110428_ciot_db_dnr.pdf.

19. **Please describe the rules for co-operation among the different bodies accessing the retained data and between these and other public authorities in detail: how is data exchange between the police and other public bodies effected under the 'Wet politiegegevens' (see your answer to question 33 of the first questionnaire)? Which rules apply to the exchange of "data retention data" between national security services and other public bodies?**

When retained data has been accessed by the law enforcement agencies, its further processing, in between law enforcement agencies and possibly to other public authorities, is governed by the Law Enforcement Data Act. Notably, there are no specific rules on the further processing of the data that are available to law enforcement as a result of blanket data retention.

Law enforcement may provide police data (including retention data it is processing) to others in accordance with Artt. 16 – 24 of the Law Enforcement Data Act. These others are specialized law enforcement agencies and other officials that have duties relating to the enforcement of the law such as mayors (Art. 16), the intelligence agencies and foreign or international law enforcement agencies to the extent there is a legal basis (art. 17), others that have legal duties that require them to structurally have access to certain police data on the basis of a weighty general societal interest (art 18), others that have legal duties that require them to incidentally have access to certain police data on the basis of a weighty general societal interest relating to the tasks of law enforcement agencies (art 19), others organizations with law enforcement has established structural cooperation relating to the tasks of law enforcement agencies in light of a weighty general societal interest (art 20), scientific researchers and statistical agencies (art 22).

Article 23 and article 24 of the Law Enforcement Data Act contain specific rules on direct access to police data for the public prosecutor's office and the national intelligence agencies respectively.

When retained data has been accessed by the national intelligence agencies, its further processing, and possible provision to other public authorities such as the police is governed by Articles 36 - 42 of the National Security Act. Notably, there are no specific rules on the further processing of the data that are available to law enforcement as a result of blanket data retention. Possible recipients include the minister of the interior, law enforcement agencies, the public prosecutor's office, and foreign or international intelligence agencies.

20. **Please provide more details about how EU legislative acts and international treaties on cross-border co-operation in data retention issues (including rules specifically designed for data retention as well as general rules applicable to data retention) are applied in the Netherlands.**

As mentioned in the previous questionnaire, there is no possibility for foreign agencies to access data held by Dutch electronic communications providers directly. In general, requests have to follow the rules for foreign requests for legal (law enforcement) assistance. Notably, there are no specific rules relating to data retained under the data retention rules. The general rules are laid down in Title X of the Code

of Criminal Procedure (Wetboek van Strafvordering). Those general rules stipulate that requests for electronic communications data have to proceed through the office of the public attorney who decides about the execution of the request (Articles 552h, 552i and 552j of the Code of Criminal Procedure).

Cross-border exchange of data for law enforcement purposes is also the subject of European Union secondary legislation, but the Framework Decision 2006/960/JHA is not applicable because retained data is considered to be information obtained by coercive means, which is outside the scope of the instrument, as can be read in the EC's official evaluation of the data retention directive.[11]

Notably, several reports suggest that the formal route through the public prosecutor's office to gain access to electronic communications data is not followed in practice. Reports suggest that many requests, in particular in border areas such as with Germany, may be dealt with informally because of the complexity of official procedures.[12]

Interestingly, the European Commission also notes that law enforcement agencies prefer to request the data of foreign (EU) subscribers directly at the operator if the operator is also present in that country.[13]

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

The Dutch legal system (i.e. the independent Courts) supervise, at the moment of trial, whether data that has been accessed in the course of a criminal procedure relating to specific crimes has been accessed legally.

The Agentschap Telecom [Radiocommunications Agency] is the administrative agency for issues related to compliance with telecommunication regulations in the broad sense. As the agency states on its website, it "*acts as the watchdog, implementer and expert across the entire domain of electronic communication*". They are the primary agency overseeing proper execution and compliance with the law. This agency is also responsible for providing industry guidance and has been

---

11 Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18 April 20011, Com(2011)225 Final, avaliable at: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

12 See e.g. J.J. Poerin, Vereenvoudigde procesgang rechtshulpverzoeken is haalbare kaart, http://spl.politieacademie.nl/vereenvoudigde-procesgang-rechtshulpverzoeken-is-haalbare-kaart/tabid/603/Default.aspx

13 Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), 18 April 20011, Com(2011)225 Final, avaliable at http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf.

actively engaged with the industry to do so in the context of data retention obligations. The Agentschap Telecom is not independent; it is an operational part of the ministry of economic affairs.

The Dutch Data Protection Authority (DPA), College Bescherming Persoonsgegevens is the independent supervising agency overseeing compliance with the Data Protection Act and the Law Enforcement Data Act. Only as a matter of funding, the Dutch DPA is part of the Ministry of Justice.

In the context of the National Security Agencies, there is an official Review Committee on the Intelligence and Security Services (Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD)) established by the Dutch National Security Act, whose task is to assess the legitimacy of the actions of the Dutch intelligence and security services. The CTIVD is independent and has far reaching powers to investigate and report on intelligence agencies' practices.

22. Does jurisprudence, academia or practice provide any guidance as to when the exemptions defined in Art. 27 Wet politiegegevens and Art. 55 National Security Act apply in data retention issues and the requested information may thus be denied?

There has been no discussion in the literature or in practice (to my knowledge) on how these restrictions would apply (differently) to requests for access to electronic communications data after they have been accessed by law enforcement or national security agencies. In fact, in the Dutch context, there is no reason to believe that these exceptions would apply differently in case the data held on a particular individual also contains electronic communications data whose access has been facilitated by the data retention system.

To be clear, the data retained as a result of the Dutch data retention directive are held by the operators and the rights to data access under the general privacy rules applies in these cases. A recent request by a Dutch activist finally (after a legal battle) resulted in the mobile operator providing access to the retained data (Comparable to Malte Spitz project).[14]

Of course, A request to access one's personal data held by law enforcement or national security agencies could be specifically directed at acquiring knowledge about whether electronic communications data are being held. In such cases the exceptions of Article 27 Wet Politiegegevens and Art. 55 National Security Act would apply.

Article 27 Wet Politiegegevens contains three different reasons not to provide access, namely when access would harm the proper tasks of law enforcement. This includes the prevention, investigation and prosecution of criminal acts as well as the public order more generally. It also includes requests that are apparently only meant

[14] Rejo Zenger, Wat verraadt de bewaarplicht over Telfort abonnees, 16 April 2011, https://rejo.zenger.nl/focus/wat-verraadt-de-bewaarplicht-over-telfort-abonnees

to burden the police. In addition to this broad exception there are exceptions in light of the weighty interests of third parties (This includes in particular data about informants.) and the safety of the state.

Article 55 of the National Security Act contains more restrictions on access. In addition, the legislature has clarified when introducing the provisions on access to one's personal data held by the national security agencies that the starting point of this system of restrictions is that the agencies can only effectively operate when a certain amount of secrecy is guaranteed.[15] Before the revision of the National Security Act, no access would be granted. The access provisions were introduced 10 years ago in reaction to case law about the right to access information under the Dutch Freedom of Information Act (Wet Openbaarheid van Bestuur). Of special importance is the restriction in view of the current level of intelligence of the agencies. When an answer to the request would reveal too much about this level of intelligence, the request can be denied (without acknowledging data are held). Of practical importance in the context of data retention is that all access to data which have been processed less than 5 years ago will be denied.

[15] Tweede Kamer, vergaderjaar 1997–1998, 25 877, nr.