

|

**Opinion from the Dutch Data Protection Authority (Dutch DPA) [College
bescherming persoonsgegevens (CBP)]
Legislative proposal (Bill) for implementation of the European Directive on
Data Retention
Pertaining to the tender letter of 22 January 2007**

TABLE OF CONTENTS

1. Retention period of 18 months	pages 1-5
1a Justification of the need for 18 months	
1b Harmonisation in the EU context	
2. The option for delegation provisions	pages 6-9
2a Types of data	
2b Centralised or decentralised storage	
2c Other delegation provisions	
3. Limitation of access to retained data	pages 10-13
3a Access for prosecutions	
3b Data mining	
3c Access for government bodies and third parties	
3d Information rights of parties concerned	
4. Resources for checking lawful use	pages 14-16
4a Statistics	
4b Obligation of notification	

1. Retention period of 18 months

Legislative proposal (Bill)

The Bill prescribes a retention period of 18 months for both telephone and Internet traffic data. The need for this period is supported in the explanatory memorandum (hereafter EM) by reference to the report *Wie wat bewaart die heeft wat* [Whoever keeps something has something] by the Erasmus University dating from 2005.¹ This report concludes that a retention period of 12 months is desirable. That period is to be regarded as a minimum according to the EM. *The retention period recommended by the researchers from the Erasmus University must however be regarded as a minimum from the perspective of efficacy of law enforcement. Bearing in mind the findings by Erasmus University, it will be less common for the retained data still to appear useful after 12 months for detecting serious criminal offences, but criminal investigations cannot be allowed to fail because that period has expired.*² The Bill also indicates that the Netherlands is not pursuing the possibility of choosing a retention period in excess of 24 months. The EM (still) lacks any explanation of the (contemplated) retention periods in other Member States. The relevant chapter 6 has been left pro memorie.

Provisions in the Directive

Article 6 of the Data Retention Directive³ offers a range of between a minimum of six months and a maximum of two years for the retention period. Article 12 additionally provides that Member States may retain the information specified in the Directive for a longer, but not unlimited, period if specific circumstances justify this.

¹ Whoever keeps something has something. Investigation into the use of and need for a retention duty for historical traffic data from telecommunication traffic (June 2005) Erasmus University Rotterdam, page 5.

² Draft Explanatory Memorandum on Amendment to the Telecommunicatiewet [Telecommunications Act] and the Wet op de economische delicten [Act on Economic Offences] in connection with the implementation of Directive 2006/24/EU by the European Parliament and the Council of the European Union, relating to the retention of data processed in connection with the provision of public electronic communications services and for amendment of Directive 2002/58/EU (Act on the obligation to retain telecommunication (traffic) data), unnumbered version, sent to the Dutch DPA with a letter of 11 December 2006, page 5.

³ Directive 2006/24/EU, relating to the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks, and for amendment of Directive 2002/58/82 (hereafter "the Directive").

1a Justification of the need for 18 months

The Dutch DPA and the Article 29 Working Party have regularly asserted the position that the introduction of an obligation to retain historical traffic data of all citizens would be a very intrusive measure, whose need would have to be demonstrated irrefutably.⁴ In article 8 of the European Convention on Human Rights (ECHR), the fundamental right of citizens is enshrined of respect for their private life. The government may only infringe on that right to the extent that it is **necessary** in a democratic society. The necessity imposes high requirements on the proportionality of each specific measure that limits the private life of citizens. The general provisions from the Directive do not alter the fact that each national implementation must be tested independently against Article 8, ECHR and the corresponding ECHR case law. This applies specifically to the need for a retention period longer than the period necessary for the commercial purpose of provisioning electronic communication networks and services.

The Dutch DPA observes that the EM hardly explains how the period of 18 months has been determined. On the one hand, the EM states that criminal investigations should not be allowed to fail because the period of 12 months has passed, and on the other hand makes reference to the retention term in other Member States. *Also, in order to prevent the creation of a disproportionate relationship in the interchange of legal assistance between the Member States in connection with the provision of retained telecommunication data, the recommendation is to opt for some extension to the retention period recommended by the Erasmus University.*⁵ Before the Dutch DPA explores the European harmonisation issue, it wishes to examine the justification, in relation to the protection of private life, for the specific need in the Netherlands for retaining traffic data for law enforcement purposes.

Bearing in mind also the proportionality of the infringing measure, the Dutch DPA points out that longer the period covered by available data, the more insight law enforcement will gain into the daily conduct of unsuspected people.

Following up the recent opinions from the Article 29 Working Party on the subject,⁶ the Dutch DPA accordingly recommends a harmonised minimum application of the provisions in the Directive, with a retention period deviating as little as possible from the original purpose for which the data are stored by providers of communication services. It is necessary to support the length of a retention obligation, which after all is at odds with the obligation to erase traffic data or make them anonymous under Directive 2002/58/EU, with convincing arguments. *"As just mentioned above, the justification for any compulsory and general data retention must be clearly demonstrated and backed up with evidence. This also applies to the maximum periods that should apply in such a case."*⁷

⁴ See on this, from the Article 29 Working Party, Opinion 4/2001 on the draft agreement by the Council of Europe on computer crime, 10/2001 on a proportionate approach to the fight against terrorism, 5/2002 on the compulsory systematic retention of telecommunication traffic data, 9/2004 on the draft framework decision [...], 4/2005 on the proposal for a Directive [...] and opinion 3/2006 on Directive 2006/24/EU. In addition, the Dutch DPA sent a letter on 2 September 2002 to the Minister of Justice on the proposal to introduce an obligation of retention; in September 2004 it made an extensive contribution to the consultation by the European Commission; an opinion article for the NRC -Handelsblad of 22 August 2005 and a contribution to the hearing of the Dutch Lower House of Parliament on 28 September 2005.

⁵ EM, page 5.

⁶ Article 29, Opinion 3/2006 and Opinion 4/2005.

⁷ Article 29, Opinion 4/2005, page 8.

With regard to such evidence, the EM bases its opinion primarily on the Erasmus University report. The Dutch DPA, however, finds that the Erasmus study provides insufficient evidence of the need for a longer retention term than is used in current practice, whereby providers retain traffic data for their own commercial purposes (i.e. for transmission and billing purposes).

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 ."*⁸

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."*⁹

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.

Even this conclusion, that a retention obligation of one year would be desirable, does not fulfil the requirement of 'necessity' in article 8, ECHR: *"(a) the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable [...]"*¹⁰ The substantiation for the proportionality demanded by the ECHR is accordingly absent.

The retention period of 18 months now being contemplated is also in stark contrast to the repeated assurances from the Minister of Justice to the Dutch parliament to the effect that the Netherlands would strive for a retention period of 12 months for telephone data and six months for Internet data. Minister Donner: *I have indicated that I wanted room for the Netherlands in any event for a retention period of one year, and a six months' period for Internet data. This has been achieved; it is possible now. If other Member States decide to incorporate longer periods in their national legislation, that is up to them.*¹¹ During this debate, a substantial majority in the Lower House approved a motion for rejection of the Directive, particularly because it allowed for the possibility of a longer retention period than 12 months.¹²

⁸ Erasmus, page 23.

⁹ Erasmus, page 23.

¹⁰ ECHR 25 March 1983, Silver and others v. United Kingdom, no. 97.

¹¹ *Official (verbatim) report II, 2005-2006, page 3405.*

¹² The motion from Dittrich and others (23490, number 407): "Bearing in mind the fact that the European Parliament and Council Directive relating to the retention of data (PE-CONS 3677/05) does not meet the conditions of a maximum retention period of one year, an adequate scheme for access to stored data and a compensation scheme for a level playing field; (...)"

Finally, the Dutch DPA notes from the EM that the retention period was apparently changed at the last moment from 12 to 18 months. A retention period of 12 months is still mentioned at three points in the text.¹³

1b Harmonisation in the EU context

Reference is made in the EM to the importance of a longer retention period than the 12 months considered in the Erasmus report as possibly being necessary in connection with requests for legal assistance from other Member States. No research has been carried out into this issue, however.

In order to increase the efficacy of international legal assistance, it seems inappropriate to look for an extension of the retention period. It would be much more opportune to look for a streamlining of procedures and formalities for international legal assistance. The same retained data may also be repeatedly asked for in long-lasting international investigations.

The most important principle of the Directive, expressed in article 1, is the harmonisation of Member States' provisions concerning mandatory data retention, in order to ensure that the data are available for the investigation, detection and prosecution of serious crime.

The Dutch DPA has only a limited insight into the implementations and proposals in other EU Member States, but is able to ascertain that there is not yet any harmonisation of retention periods. Our neighbour, Germany,¹⁴ is opting for a retention period of six months, just like Finland and the Czech Republic¹⁵. Sweden, one of the four Member States who took the initiative for the creation of the European obligation of retention, appears also to be opting for a minimal implementation. Other countries such as France,¹⁶ Denmark¹⁷, Spain¹⁸ and Belgium are opting for a retention period of 12 months. Only Italy¹⁹ and Ireland²⁰ have longer periods, of 4 ½ years and three years respectively.

¹³ EM, page 10, page 20 and page 32. Page 10: (...) will be retained for nine months more (than the average of three months). Page 20: The retention period proposed in this Bill coincides with the period recommended by the Erasmus University. In light of interests involved, the proposed period can hardly be faulted for being disproportionate. Page 32: The obligation for destruction implies that as soon as one year has passed from the date of this Bill entering into effect, the retained data will start to be erased on a day by day basis.

¹⁴ The German Bill with its explanatory memorandum has been subject to consultation since 8 November 2006. Bill URL: http://www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/de-recht/RefETeil1neu.pdf Explanatory memorandum URL: http://www.humanistische-union.de/fileadmin/hu_upload/doku/vorratsdaten/de-recht/RefETeil2neu.pdf

¹⁵ Order by the Czech telecommunications authority (CTÚ), mid December 2005. The order prescribes retention periods of between three and six months. English-language information: <http://www.ctu.cz/main.php?pageid=178>

¹⁶ France: Décret n° 2006-358 du 24 mars 2006 d'application de la loi sur la sécurité quotidienne (LSQ), relatif à la conservation des données de communication, URL: <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=JUSD0630025D>

¹⁷ Denmark: Executive Order (988/2006), URL: <http://www.jm.dk/image.asp?page=image&objno=76136> and Guidelines (174/2006), URL: <http://www.jm.dk/wimpdoc.asp?page=document&objno=76135>, both of 28 September 2006. Both come into effect on 15 September 2007.

¹⁸ Spain has framework legislation enabling mandatory Internet data retention for 12 months, but no concrete delegation provisions nor any obligation to retain telephony traffic data. Ley de Servicios de la Sociedad de la Información (LSSI), operational since 12 October 2002, URL: <http://www.lssi.es/>

¹⁹ Since 2003, via Decree 259/2003, 'Codice delle comunicazioni elettroniche', Italy has had an obligation to retain telephony traffic data for 30 months, with a possibility for extension by 24 months, and an obligation to retain Internet traffic data for six months, with a possibility of a further six months' extension. The decision was taken (article 6) at the end of July 2005 to retain all traffic data including Internet data until 31 December 2007, Nuove norme per il contrasto del terrorismo internazionale e della criminalità, in *working sinds 1 augustus 2005*, URL: <http://www.interno.it/legislazione/pages/articolo.php?idarticolo=646>

The Dutch DPA does not know whether the Commission has already pronounced any opinion on the extra long periods in these three countries, or on the specific circumstances that might justify these longer retention periods.

Finally, in the United Kingdom - the major driving force behind the introduction of a European obligation to retain traffic data, certainly following the attacks of 7 July 2005 – the retention measures are, for the time being, confined to voluntary arrangements with a large number of operators. For some time now, the affiliated operators have been providing the data asked for upon payment of the full costs involved. The United Kingdom has in fact had the legal possibility to introduce statutory data retention since the end of 2001.²¹

Given the importance of protecting personal data, and the obligatory weighing of the balance between the rights of citizens and the need for governments to infringe on (of upon?) these rights in specific circumstances, the Dutch DPA attaches great value to the German option for a minimum implementation of the Directive.

The German option for a minimal retention period was motivated by consistent opposition by Parliament to the introduction of mandatory data retention. This opposition was partly inspired by research by the sector organisation Bitkom into the use of and need for the retention of traffic data. The research compares legislation and the use of historical traffic data in Austria, France, Italy, the Netherlands, Sweden, Spain, the United Kingdom and United States. This report also concluded that a retention period of more than (on average) three months could not be justified.²²

Summary

The Dutch DPA considers that the Netherlands must suffice with the minimal obligatory retention period of six months, which is in many cases longer than the period for which the data are required for regular business purposes (transmission and billing). No use or necessity for a longer retention period have been demonstrated. Any reliance on the need for harmonisation of the periods must also fail, considering the major differences in implementation in different Member States.

²⁰ Ireland only has an obligation to retain telephony traffic data. Irish Criminal Justice (Terrorist Offences) Act, 2005, Part 6, paragraph 63, URL: <http://www.irishstatutebook.ie/ZZA2Y2005S63.html>

²¹ The legal possibility to introduce an obligation to retain traffic data is established in the Code of Practice on Data Retention, incorporated as Part 11 of the Anti-terrorism, Crime and Security Act. URL: <http://security.homeoffice.gov.uk/ripa/communications-data/data-code-of-practice/> The accompanying (reviewed) draft Code of Practice of 10 March 2005 does not set out any retention period, but only the access facilities. URL: <http://security.homeoffice.gov.uk/ripa/publication-search/ripa-cop/acquisition-disclosure-cop.pdf?view=Standard&pubID=401821>

²² Summary of BITKOM research (in German, October 2004), URL: http://www.bitkom.org/files/documents/Zusammenfassung_Studie_VDS.pdf; URL of complete report: http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf

2. The option for delegated provisions

Legislative proposal (Bill)

In converting the provisions of the Directive, the Bill opts to postpone five important decisions and to confine itself to undefined delegated provisions (administrative decrees), particularly relating to the types of data to be retained, the choice for either centralised or decentralised storage and the maintenance of statistics on the use of the data. In addition, the prescribed security measures are also delegated to an administrative decree (NB: in the Netherlands an administrative decree is generally not discussed in Parliament) that has yet to be prepared, along with the interpretation of the way in which and the speed with which providers should be able to comply with requests.

Provisions in the Directive

In article 5, the Directive prescribes in detail which categories of data have to be retained. According to note 12 of the Directive, this list is to be understood as being a maximum. If they want to retain other data (such as data relating to unconnected calls) the Member States may rely on article 15.1 of Directive 2002/58/EU. Any legislation announced on the basis of that article must additionally comply with the requirement that the legislation *constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system as referred to in article 13.1 of Directive 95/46/EU.*²³

As regards the choice between centralised and decentralised storage, consideration 13 of the Directive states that duplication of the retained data must be avoided.

2a Types of data

The choice to include the types of data in an administrative decree rather than in the text of the Act itself does not correlate with the choice made in the Directive on the data to be retained. The European Commission originally proposed adding a list of data as an annex to the Directive. This would also involve a separate, accelerated decision-making procedure (described as "comitology") for adjustments to the list. The European Parliament accepted, by a large majority, an amendment from the liberal rapporteur Alexandre Alvaro to include the information in the text of the Directive itself. This included the explicit choice to create a more demanding procedure to adopt any changes of the categories of data to be retained, with full approval rights on the part of the European Parliament.

The Dutch DPA infers from the legislative notes (LN, instructions on the process of creating legislation)²⁴, and particularly from the explanation to note 22, LN, that the principal elements of a Directive must be incorporated in the Act itself, and that "*as regards what extent of delegation is permissible, there must always be a check on which elements of a regulation are so weighty that the people's representative body (i.e. parliament) must be directly involved in establishing them.*" It is clear that the list of data to be retained is a principal element of the legislation, so that the primacy of the legislature

²³ Directive 2002/58/EU, article 15.1.

²⁴ Government Gazette 1996 page 177.

should take precedence. The Dutch DPA considers that the German Bill provides a good model for this type of implementation.²⁵

Information on location during the communication

It appears from the Explanatory Memorandum that the Netherlands wish to go further in the proposed delegation provisions than the types of information prescribed in the Directive. Providers would also have to retain the location data (from mobile telephones and, for example, laptops and PDAs using mobile data communication) arising *during and at the end of the communication*.²⁶ According to the EM, this would only amount to an extension of the existing obligation under the present Decree on Extraordinary Collection of Phone Number Data. The Dutch DPA is of the opinion that this is an incorrect reading of the obligation in that Decree. The Decree was passed in order to create a way to obtain the identity of the user of a prepaid mobile telephone in preparation of a lawful interception order. In such cases, the law enforcement authorities indicate to the provider the times (at least two) and the locations from which a mobile phone have been used. The operators can only be asked to retrieve the location information to the extent that they process the information. The Decree explicitly does not contain any obligation to collect information and accordingly does not create any obligation to retain all location information during communications for three months. In practice, providers must only retain information concerning the cell ID at the start of the communication.²⁷

According to the Dutch DPA, retaining location information during the communication is excessive in regard to the Directive, and as a proposed delegated provision, such retention is in conflict with Note 337, LN. This note stipulates that, when implementing a Directive, it is not permitted to include rules other than those necessary for implementation.

But even if this extra category were to be incorporated in a separate legislative proposal, relying on the exception facility in article 15.1, 2002/58/EU, the Dutch DPA considers that the retention of this category of information is disproportionate. This category was excluded, with good reasons (or: strong arguments), from the Directive, because it amounts to an overly intrusive, far reaching and secretive surveillance of the movements of very large numbers of unsuspected citizens. The German explanatory memorandum refers explicitly to the debate in the European Parliament on this topic, and confirms that the Directive is proportional precisely because this type of information does not need to be retained.²⁸

²⁵ In the new section 110a of the Telekommunikationsgesetz (TKG), "Speicherungspflichten für Verkehrsdaten", subsection 2 provides a specification of the traffic data to be retained from fixed, mobile and Internet telephony services, subsection 3 provides a specification of the e-mail traffic data and subsection 4 provides a specification of the traffic data in relation to Internet access.

²⁶ EM, page 4: "For the category of location data, it will be determined - notwithstanding the Directive - that the location data generated after the start of the communication will also have to be retained" and at page 7: "This data analysis is elaborated in the Decree on Special Collection of Number Data (Bulletin of Acts, Orders and Decrees 2002, 31). The provider is obliged to retain the information required for the data analysis for a period of three months. What is involved here is the data relating to the times when telecommunications have taken place, the numbers corresponding with those times and with the relevant telecommunication and the base stations (cells) where the information was received." (...) This implies that the retention period of three months will be increased to 18 months for the required data."

²⁷ Taken from the Joint Response by Providers to the consultation on the Data Retention Bill, page 5.

²⁸ German Begründung, page 64: "(...)insbesondere da besonders kostenträchtige Speichervorgaben auf europäischer Ebene verhindert werden konnten (z.B. Speicherung „erfolgloser Anrufversuche“, auch wenn diese von den Diensteanbietern bisher nicht gespeichert oder protokolliert werden; Speicherung von Standortdaten auch während und am Ende von Mobilfunkverbindungen)."

2b Centralised or decentralised storage

Consideration 13 to the Directive prescribes that the data must be retained in such a way *to avoid their being retained more than once*. This consideration excludes Member States from choosing a model for the retention obligation similar to the CIOT (Centraal Informatiepunt Opsporing Telecommunicatie) in the Netherlands [Central Information Point for Telecommunication Research]. This is a system in which telephone and Internet providers copy the names, addresses and residence details of their customers to a separate server that can be consulted via the CIOT. The competent authorities can query all providers at the same time via the CIOT in order to obtain the identity of the user of a particular number or, vice versa, the number pertaining to a particular identity. The Minister of Justice repeatedly indicated, during debates in the Lower House and in letters, that he preferred a CIOT-type solution for the implementation of the retention obligation.²⁹ In so doing, he left open the possibility as to whether the data would have to be duplicated or immediately passed to a central server park. The Dutch DPA confirms that, if a CIOT-type solution is chosen, there will always be a duplication of a particular set of data, namely the data required for the provider's own business purposes (three to six months depending on, for example, invoice periods). The Dutch DPA considers that the duplication of this set of data is in conflict with the Directive.

Following the recommendations by the Article 29 Working Party, the Dutch DPA recommends a *decentralised, logically separate* storage of the traffic data to be retained specifically for law enforcement purposes. One way or another, different rules will apply to the data to be retained under section 13.2a of the Telecommunicatiewet (Tw) [Telecommunications Act] for retention, use, hand-over, security and erasure. A provider cannot achieve this without separating this data logically from the data processed for its own business purposes.

The Explanatory Memorandum also refers to research carried out by Verdonck, Klooster & Associates BV. This report concludes that central storage of the data would be preferable, based on cost considerations and because the data would be easier to secure. The results of this research, however, are not enough of a basis for making a choice between centralised or decentralised storage according to the Explanatory Memorandum. The Dutch DPA infers, from the the joint response to the consultation on the Bill by virtually all telephony and Internet providers in the Netherlands³⁰, that the providers are unanimously distancing themselves from the conclusions of the above-mentioned research, particularly as regards any preference for centralised storage.

The Dutch DPA considers that the report wrongly fails to take into account the risks involved in centralised storage, such as additional uses not yet foreseen. The experience of the Dutch DPA is that every supply creates its own demand.

²⁹ For example in the submission letter with the Erasmus report, Parliamentary Documents II, 2004-2005, 23490, no. 388, page 7: "The CIOT model has many benefits including cost effectiveness. This model is significantly less expensive than the model under which providers are obliged to develop separate systems to comply with the obligation of retention. For the providers, the benefit of applying the CIOT model is the fact that the CIOT retains, organises and queries the information."

³⁰ Joint Response by Providers to the consultation on the Data Retention Bill, sent to the Minister of Economic Affairs on 18 January 2007.

Decentralised storage, on the other hand, has an important benefit not recognised by the Explanatory Memorandum, namely that the providers will carry out an extra check on whether or not a request can be answered. Experiences with the introduction of new criminal investigation powers in the telecom sector demonstrate that there is a need for a great deal of consultation on exactly how questions are asked, and the possible answers. The report from the University of Tilburg on the evaluation of seven years of lawful interception policy “*recommends investment in knowledge and expertise on the shop-floor (not **only** for, but certainly **primarily** for, those asking the questions)*”³¹ Experiences with lawful interception indicate the need for considerable restraint in connection with the desire to computerise search queries through the complex databases holding historical traffic data. Extra processing is frequently required in order to supply a careful answer. The expertise of the providers may prove to be indispensable in this.

2c Other delegated provisions

The Dutch DPA fails to understand why the obligation to provide statistics, as prescribed by the Directive in article 10, has not been converted into the text of the Bill itself. The Dutch DPA will explore this in greater detail when discussing resources to control the lawful use of the data.

As regards the security measures rendered obligatory by the Directive, the Dutch DPA can imagine that delegation would be useful, since detailed technical specifications are involved. The nature of this delegation however is not optional and it must therefore be interpreted in greater detail in the EM.

Finally, and concerning the possible delegated provision (administrative decree) on the interpretation of the criterion of “without undue delay”, as contained in the Directive to meet a request for traffic data, the EM refers to *the current arrangements at an operational level agreed between the providers and those agencies asking the questions.*³² The Dutch DPA considers it important that the EM explains that these current arrangements cover a period of between one and five working days, depending on the processing required by a provider in order to produce the data that have been requested.

Any administrative decree to be drafted with a more detailed interpretation of the periods should in any event reflect practice among major and minor providers, without compulsorily imposing on all providers a transmission time available from one specific provider.

Summary

The Dutch DPA considers the option of including in delegated provisions the types of data, the method of storage and the obligation to keep statistics updated, to be undesirable and incorrect from a technical legislative perspective. When establishing the types of data, the text of the Act should limit itself to the data prescribed in the Directive. Expansion of the obligation to retain data generated *during the communication* can only be submitted as a separate legislative proposal after it has been tested independently against the requirements of article 8 of the European Convention

³¹ Koops, B., R. Bekkers, F. Bongers & M. Fijnvandaat. Evaluation of lawful interception policy, An evaluation of chapter 13 of the Telecommunicatiewet [Telecommunications Act], Tilburg, November 2005, page 9.

³² EM, page 12.

on Human Rights. The proposal to adopt substantive elements of the regulation in delegated provisions is also in conflict with Note 22, LN. The fact that the EM leaves open the choice for centralised or decentralised storage is in conflict with consideration 13 of the Directive. The Dutch DPA considers decentralised storage with a strictly logical separation of the operational data to be unavoidable.

3. Limitation of access to retained data

Legislative proposal (Bill)

According to the explanatory memorandum the obligation to retain data is designed to ensure that the data will be available for investigating, detecting and prosecuting serious crime. As regards access to the retained data, section 11.13, paragraph 2 of the Telecommunicatiewet (Tw) [Telecommunications Act] prohibits providers from processing data retained under section 13.2a paragraph 2 for any other purposes. According to the EM, this accordingly ensures that the data to be retained under chapter 13 of the Telecommunications Act will be retained exclusively for a different purpose than under Chapter 11, namely to have it available for combating serious crime.

The data to be retained in terms of section 13.2a may not be processed by a provider for its own business purposes unless they are data that may already be processed in terms of sections 11.5 and 11.5a of the Tw [Telecommunications Act].

The EM points out that the various supervisory bodies are free to request the data they require for their own duties. This option is only available for the data retained by the provider in accordance with sections 11.5 and 11.5a of the Tw for their own business purposes.³³ The data retained under chapter 13 will not, for example, be accessible by OPTA [Independent Post and Telecommunications Authority].³⁴

The EM also provides an overview of current legislation that can be used to subpoena data for law enforcement and the prosecution of criminal offences. The CIOT remains the gateway to request telecommunications subscriber data.

Provisions in the Directive

The basic principle is that the data to be retained are available for investigating, detecting and prosecuting serious crime as defined in national legislation within the Member States (article 1, paragraph 1). In article 4, the Directive specifies that the Member States must ensure that the data retained in accordance with the Directive will only be provided to the competent authorities in specific cases and in accordance with national law. Legislative measures governing access to and use by national bodies do not, according to consideration 25, fall within the scope of Community law.

The need for restrictions concerning access

The Dutch DPA and the Article 29 Working Party have consistently pressed for specific safeguards in the implementation of the Directive in national legal systems, in

³³ EM, page 10.

³⁴ Idem.

order to meet the requirements posed by article 8 of the European Convention on Human Rights. Restricting access has always been a source of concern in this area. Again and again, the need has been indicated to confine access to the retained data to the detection, investigation or prosecution of *serious* crime. Processing for other purposes ought to be specifically excluded, as should the possibility of data mining on the communication and movement patterns of unsuspected individuals.³⁵

Article 4 of the Directive obliges Member States to adopt the procedure and the conditions to be fulfilled for access to the retained data in national law, bearing in mind the relevant provisions of European Union legislation or public international law, particularly the European Convention on Human Rights as interpreted by the European Court of Human Rights. The fact that the Directive explicitly uses the term "law" for this subject, in relation to the ECHR, and not a general term such as "measure", obliges the Member States to provide for strict access limitation in the text of the Act itself.

The present Bill only partially meets these requirements. The point that providers are banned from using the traffic data retained specifically for law enforcement purposes for their own purposes **is well made**. The Dutch DPA cannot, however, see any clear restriction in the purposes for which the retained data can be made available to law enforcement bodies and intelligence agencies. The proposed section 13.2a admittedly formulates the purpose for which providers must retain the data, namely to investigate, detect and prosecute serious offences, but this obligation only excludes further processing for their own business purposes.

The proposed provision in section 11.13 of the Tw [Telecommunications Act] does not, in the view of the Dutch DPA, in any way hamper the exercise of the already existing powers to request access to data, not only by law enforcement but also by other administrative bodies. The Dutch DPA also assumes that the present Bill was not intended in any way to introduce changes to the possibility for third parties to obtain access to retained data under civil law on the basis of section 13.2a Tw. The Dutch DPA accordingly considers that the Explanatory Memorandum is wrong in concluding that Dutch legislation provides adequate procedures and safeguards for access by the competent national authorities to the retained data.

3a Access for criminal proceedings

There is a noticeable difference between the texts of the Act and the EM in relation to access for criminal proceedings. In new paragraph 1 of section 13.4 of the Telecommunicatiewet, sections 126n and 126u of the Wetboek van strafvordering (Sv) [Dutch Code of Criminal Procedure] and section 28 of the Wet Inlichtingen- en Veiligheidsdiensten [Intelligence and Security Services Act] are mentioned as the basis for requests with which the providers must comply. But the EM also mentions sections 126na and 126ua of the Sv, as well as the powers granted under the Wet terroristische misdrijven [Terrorist Offences Act] in sections 126ii, 126hh and 126zh and 126 zi, Sv.³⁶

The Dutch DPA considers that the law must provide a limitative summary of facilities for access under criminal law, both in the text of the Act and in the EM. Special

³⁵ Section 29 WP, opinion 3/2006

³⁶ EM, page 15.

attention must be paid to the existing section 13.2b of the Tw, which is not amended in the current Bill. It would be preferable, in the view of the Dutch DPA, to amend the relevant criminal law powers and then to make the mirror provisions in the Tw (and particularly section 13.2b and proposed section 13.4 .1) coincide with them.

In the light of the (imminent) retention obligation, the Dutch DPA considers it necessary to carry out a critical assessment of the system of applicable criminal law powers. In so doing, the Dutch DPA fails to see what added value is supplied by the freezing order in section 126ni, Sv. It was decided in the German implementation proposal not to introduce this provision from the Cybercrime Treaty, because the retention obligation already provided for the possibility of keeping up-to-date traffic data available for criminal investigation purposes.

3b Data mining

Section 126hh, Sv, provides the power to demand all retained data or parts thereof with a view to preparing an investigation into terrorist offences. The Dutch DPA considers that the application of this power to the data covered by the retention obligation would be in conflict with article 4 of the Directive. This article requires the Member States to adopt provisions to ensure that data is only issued in specific cases.

In this context, the Dutch DPA refers to the judgment by the Bundesverfassungsgericht [German Constitutional Court] of 4 April 2006³⁷. The Court held that preventive '*Rasterfahndung*', without any actual indications of immanent danger, involved an unallowable infringement of the private life, while data mining has to be regarded as being unsuitable for averting any such danger, if only because this method requires a great deal of time. According to the Dutch DPA, the current Bill therefore should exclude section 126hh from being applied in order to obtain a (partial) file of all retained data.

3c Access for government bodies and third parties

The EM does not make it clear whether a provider can or ought to refuse to comply with a request from an administrative body or civil requests from third parties to provide data retained under section 13.2a of the Telecommunicatiewet (Tw).

The EM specifically mentions the OPTA, which should be able to access the data retained by a provider in accordance with sections 11.5 and 11.5a of the Tw, but other administrative bodies might start to invoke their own powers to claim access to the data. This might give rise to complex questions relating to the priority of competing laws.

The new section 11.13 of the Tw prohibits providers from processing retained data for purposes other than the detection and prosecution of serious crime. It can be anticipated that these provisions will clash with potential claims by administrative bodies or orders by the Courts. It is not for the provider to find the correct path, but for the legislator. The Dutch DPA accordingly considers that the current Bill should explicitly exclude the possibility of retained data being obtained through administrative law or civil law channels. This can be done by amendment of the

³⁷ BvR 518/02; for a discussion, see also *Datenschutz und Datensicherheit* 30 (2006) 11, pages 685 et seq.

relevant powers, for example, in the case of the OPTA, via section 18.7 of the Telecommunicatiewet.

3d Information rights of data subjects

In the fifth chapter, Protection of Rights, the EM explores the right to get an overview of personal data processed about the data subject. The right to access, as defined in section 35 of the Wet bescherming persoonsgegevens (WBP) [Dutch Data Protection Act] is considered to be applicable in full. If asked, providers must supply a complete summary of the retained data, without being able to rely on the grounds of exception in section 43a and 43b WBP. The right to correction, as defined in section 36 WBP should also be applicable.

The Dutch DPA applauds every explicit acknowledgement of the information rights of data subjects, but considers that a more detailed balancing of the interests of third parties will have to be carried out on a case-by-case basis, as specified in section 43e, WBP. Third parties are inevitably involved when examining traffic data concerning telecommunications, namely those individuals whom the party concerned has phoned or e-mailed. The provision of an extensive summary (which might go back as far as 18 months in terms of the current Bill) may be an infringement of the rights and freedoms of individuals other than the data subject. In addition, a subscriber might be able to gain detailed insight into the communication conduct or location data of all users over a lengthy period. This might, for example, involve employees or family members, including minors. The EM wrongly fails to deal with this problem area.

This problem with the right of access would hardly have occurred at all if the retention periods opted for had been equal to the (limited) period for which data were retained for business purposes. There are, after all, solutions available for both mobile and fixed telephones in order to protect privacy, such as preventing the presentation of the calling line identification (number). This does not, however, apply to the Internet. For the delivery of e-mails no specified invoices are sent, and there are accordingly no solutions available for withholding address details.

Summary

The Dutch DPA considers that the limits for access to the data to be retained have not been drawn clearly enough. This means that the current Bill is in conflict with article 4 of the Directive. The Dutch DPA wonders to what extent section 11.13 of the Telecommunications Act limits the existing options for third parties to gain access to the retained data. The existing legal powers for accessing the retained data must therefore be limited still further. This applies not only to the criminal law powers but also to administrative law and civil law powers.

The Dutch DPA recommends that the current Bill should also exclude the power under section 126hh, Sv, from being potentially applied to obtain (parts of) all retained data (for data mining purposes).

The system of criminal law powers under which the law enforcement agencies can access the retained data needs further critical consideration, particularly as regards the relationship between the retention obligation and the quick freeze of traffic data

(section 126ni, Sv).

In relation to the information rights of data subjects, the Dutch DPA recommends the inclusion in the EM of an extensive explanation of the balance to be struck with the fundamental rights of others, particularly in relation to employees and family members.

4. Checks and balances on lawful use

Legislative proposal (Bill)

The transposition table with the current Bill indicates that article 10 of the Directive, concerning the provision of annual statistics to the European Commission relating to requests for data and usage, has not been incorporated. The EM indicates that providers must keep the statistics.³⁸ The Public Prosecutor may maintain a record of this. *Recording of this data can be coordinated by a body to be appointed by the Minister of Justice. This might, for example, be the National Office of the Public Prosecutor.*³⁹ The Bill assumes that the statistics will only relate to judicial requests: *As regards the data requested by the intelligence and security services, the position is that the information on the application of these powers by the services is a state secret.*⁴⁰

Provisions in the Directive

Article 10 of the Directive prescribes that the Member States must provide statistics to the European Commission on an annual basis concerning the number of cases and time elapsed, including those cases in which the request for data could not be met.

4a Statistics

The obligation to keep statistics is included in the Directive in order to be able to assess, after a period of time, whether the Directive is adequate or needs further adjustment, as regards both the categories of data and the retention period. The Dutch DPA considers that the evaluation provisions in the Directive mean that the statistics will be made public, at least partly, when the European Commission presents a public evaluation report to the European Parliament and Council not later than 15 September 2010.⁴¹ Bearing in mind the major social importance of mandatory data retention, the Dutch DPA considers that the legislature must also carry out its own evaluation of the implementation eventually opted for. It would benefit such an investigation if public statistics were available on the number of requests for historical traffic data. Tying in the provisions from the Directive regarding statistics in the Act will also enable the (obligatory) publication of statistics on the number of wiretaps, as promised by the government in a letter of 15 December 2006.⁴² Any such obligation to maintain statistics on the part of the National Office of the Public Prosecutor could follow the model of the German implementation proposal at paragraph 100g.⁴³ The Dutch DPA

³⁸ EM, page 30. "These data will have to be collated by the providers (...)".

³⁹ EM, page 31.

⁴⁰ *Idem*.

⁴¹ Directive, article 14.1.

⁴² *Parliamentary Documents II* 2005/06, 30 517, no 2, page 13: "The Government is certainly prepared to maintain tapping statistics as regards taps in the interests of investigating criminal acts, and to be politically accountable for this."

⁴³ SPO-E Penal Code § 100g [Erhebung von Verkehrsdaten]
(4) *Über Maßnahmen nach Absatz 1 ist entsprechend § 100b Abs. 5 jährlich eine Übersicht zu erstellen, in der anzugeben sind:*

1. die Anzahl der Verfahren, in denen Maßnahmen nach Absatz 1 durchgeführt worden sind;

agrees with the German legislators that the obligation should be imposed on those issuing the requests rather than on the providers.

The EM states that a record is kept via the CIOT of requests for subscriber data, but that this is not the case for the exercise of other criminal law powers at the moment. As regards requests via the CIOT, the Dutch DPA wants to point out that very large numbers are involved, and that since it was set up in 1999, no audits into the lawfulness of the provision of data have taken place, in spite of the obligation to do so contained in the Besluit verstrekking gegevens telecommunicatie [Decree on the Provision of Telecommunication Data].

Finally, the Dutch DPA considers that the Directive draws no distinction, in relation to the statistics to be supplied, between requests by intelligence services and judicial requests. The Directive talks about "competent authorities". The Dutch DPA does not understand how mentioning a number (the number of requests by the intelligence services) might jeopardise any state secret.

4b Obligation to notify

Nothing is said in the draft Bill on the obligation to notify in case of requests of data other than identifying data. The Dutch DPA considers that compliance with the obligation to notify and the maintenance of statistics on the number of notifications are important to enable a check to be made on the lawful use of the data. This obligation to notify was introduced with the introduction of the Wet bevoegdheden vorderen gegevens [Data Delivery Act], as an important safeguard: *These safeguards promote the careful application of the powers, and are accordingly also in the interests of individuals in relation to whom data is requested in the interests of a criminal investigation.*⁴⁴

During the Senate debate on this Act, the members referred to a report from the Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) [Research and Documentation Centre] showing that the obligation to notify had been infringed on a large scale. The Minister then indicated: *Because the obligation to notify is indeed one of the safeguards for a careful and auditable application of the special investigation powers, a better application of this obligation is important. The public prosecutor has accordingly been asked, in relation to the assessment of the Wet bijzondere opsporingsbevoegdheden [Special Investigation Powers Act] to prepare a plan of action, including measures designed to achieve better compliance with that obligation.*⁴⁵

One way of promoting better compliance with the notification obligation would be to set up an obligation to maintain statistics relating to the issuing of notifications. These statistics should also include the number of cases in which the subjects were deliberately not notified, with appropriate reasons. Here, too, the Dutch DPA regards the German implementation proposal as providing a relevant model.⁴⁶

2. die Anzahl der Anordnungen von Maßnahmen nach Absatz 1, unterschieden nach Erst- und Verlängerungsanordnungen;

3. die jeweils zugrunde liegende Anlassstraftat, unterschieden nach Absatz 1 Satz 1 Nr. 1 und 2;

4. die Anzahl der zurückliegenden Monate, für die Verkehrsdaten nach Absatz 1 abgefragt wurden, bemessen ab dem Zeitpunkt der Anordnung;

5. die Anzahl der Maßnahmen, die ergebnislos geblieben sind, weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren

⁴⁴ Parliamentary Documents I2004/05, 29 441, no C, page 12

⁴⁵ Parliamentary Documents I2004-05, 29 441, no C, page 15

⁴⁶ § 101 SPO [Allgemeine Verfahrensregelungen bei verdeckten Ermittlungsmaßnahmen]

Von den in Absatz 1 genannten Maßnahmen sind die nachfolgend bezeichneten Personen zu benachrichtigen, soweit diese bekannt sind oder ihre Identifizierung ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht

Summary

The Dutch DPA recommends to the legislature that it should establish the obligation to maintain statistics in the text of the Act itself, and obliges itself at the same time to publish the statistics. These should also include the numbers of requests by the intelligence services. In order to increase the resources available for supervising the lawfulness of requests, the Dutch DPA also recommends strict compliance with the obligation to notify, linked with an obligation to maintain statistics concerning compliance with that obligation

überwiegende schutzwürdige Belange anderer Betroffener entgegenstehen. Dabei ist auf die Möglichkeit nachträglichen Rechtsschutzes nach Absatz 9 und die dafür vorgesehene Frist hinzuweisen. Zu benachrichtigen sind im Falle (... verschiedene wetsartikelen)

6. des § 100g [Verkehrsdatenerhebung] die Beteiligten der betroffenen Telekommunikation § 100^e [Berichtspflicht]

(1) Für die nach § 100c angeordneten Maßnahmen gilt § 100b Abs. 5 entsprechend. Die Bundesregierung berichtet dem Deutschen Bundestag jährlich über die im jeweils vorangegangenen Kalenderjahr nach § 100c angeordneten Maßnahmen

(2) 8. ob eine Benachrichtigung der Betroffenen (§ 101 Abs. 4 bis 7) erfolgt ist oder aus welchen Gründen von einer Benachrichtigung abgesehen worden ist.