

Brussels, 16 September 2002

ROOM DOCUMENT No. 7

Multidisciplinary Group on Organised Crime
(Brussels, 16 September 2002)

Greece, Luxembourg and Portugal were not in a position to provide the answers to the questionnaire until the MDG meeting because the matter was currently under consultation within the administrations.

France has provided a preliminary answer but it was not possible to include it as had to be verified by the French ministries that were involved in answering the questionnaire.

The replies will be presented to the MDG at a later stage.

Subject: Item 5 b on the agenda:
Presentation by the Presidency of answers to questionnaire on retention of traffic data doc. 11490/1/02 CRIMORG 67 TELECOM 4 REV 1

Country	Answer
Austria	Under Section 93 of the Law on Telecommunications (TKG), exchange data may not in principle be stored and must immediately be erased or made anonymous by the service provider when the call is terminated (paragraph 1). Only to the extent necessary for subscriber billing should the provider store exchange data until expiry of the deadline for legally contesting the bill or asserting a claim to payment (paragraph 2). The term "exchange data" covers active and passive subscriber numbers, the address of the subscriber, the type of terminal, the charge code, the total number of units for the billing period, the type, date, time and duration of the call, the amount of data transmitted and any other payment information (Section 87(3), point 5 of the TKG).
Belgium	By adopting the Computer Crime Act (28 Nov. 2000) [Loi sur la criminalité informatique], Belgium has settled the principle of compulsory data retention for

<p>Question 1:</p>	<p>Has your country at present any special legislation concerning traffic data retention or is data traffic retention covered by existing legislation? If not are you considering legislation concerning traffic data retention?</p>
	<p>telecommunications service providers in order to make it available, if necessary, for a criminal investigation. The legislation has entered into force, but will only have effect after its implementation through a specific regulation to be adopted by the government.</p>
<p>Denmark</p>	<p>The current Danish legislation on retention of traffic data can be found in Act No. 418 of 31 May 2000 on Competitive Conditions and Consumer Interest in the Telecommunications Market and in Executive Order No. 1169 of 15 December 2000 on the Provision of Telecommunications Networks and Telecommunications Services.</p> <p>At present the telecommunications companies and Internet service providers are under no obligation to log any traffic data. According to section 30 and annex 1 of the Executive Order mentioned above they are allowed to log certain data which is needed for the purpose of end-user billing or interconnection payments. The traffic data that can be stores for these purposes are:</p> <ol style="list-style-type: none"> 1. telephone number or identification number of the end-user terminal, 2. address of the end-user and the type of terminal, 3. total number of units to be charged for the accounting period, 4. called number, 5. type, starting time and duration of the calls made and/or the data volume transmitted, 6. date of the call/service, and 7. other information concerning payments such as advance payment, payments by instalments, disconnection and reminders. <p>Such storing and processing shall be permissible only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued. These rules implements article 6 of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector which will be replaced by a similar article in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).</p> <p>By Act No. 378 of 6 June 2002 (The Anti-Terrorism Act of the Ministry of Justice), the Danish Parliament passed some amendments to inter alia the Danish Administration of Justice Act in order to improve the investigative possibilities of the police. A main element of the act is the insertion of a provision into section 786 of the Administration of Justice Act, according to which telecommunications companies and Internet service providers have to record and store ("log") for one year the information on tele and Internet communications of relevance to police invasion of the secrecy of communications etc.</p> <p>The recording and storage only concern traffic data and not the actual contents of the communication (content data). Furthermore, only the companies have a duty to record and store the traffic data in question. The rule does not involve extended police access to these data.</p> <p>The insertion of the provision in section 786 of the Administration of Justice Act has not yet come into force. The detailed (technical) rules on this logging will be prescribed by the Minister of Justice following negotiations with the Minister of Science, Technology and Innovation and otherwise following a dialogue with the industry.</p>

Question 1: Has your country at present any special legislation concerning traffic data retention or is data traffic retention covered by existing legislation? If not are you considering legislation concerning traffic data retention?	
Finland	<p>Data traffic retention has been covered at the Finnish Data Protection Law. By default a communications service provider (CSP) must either destroy or alter retained traffic data in such a way that communicating individuals can't be identified afterwards. A CSP may retain logs for a maximum period of three years, should it be necessary for either business (invoicing, marketing) or data security related tasks. If a CSP is selling services, it must keep the traffic data for a minimum of three months for invoicing purposes. Other than that, there is no obligation to retain any data traffic.</p> <p>There is also Act and Decree on the Protection of Privacy and Data Security in Telecommunications (565/1999) (For the Act, see annex). In addition, the Coercive measures Act (450/1987) has sections concerning telecommunications monitoring as well as the duty of service providers to assist and the duty to pay compensation to the service provider.</p>
France	
Germany	<p>In Germany traffic data retention is covered by existing legislation. As far as service providers are concerned, a distinction is made between "teleservice providers", covered by the law on teleservices (TDG), and "suppliers of telecommunications services", covered by the law on telecommunications (TKG). Currently, the parties named in those laws (eg. telecommunications undertakings, Internet providers) have the right, but are not obliged, to retain traffic data for a maximum of six months. Pursuant to section 89, paragraph 2, of the TKG, section 7 of the telecommunications data-protection Regulation (TDSV) and section 6 of the teleservices data-protection law, traffic data may be retained only for the purposes of tendering an account or for the submission of a claim for compensation by the service provider in the event of a suspected failure to supply services. It may also be retained, pursuant to section 89, paragraph 2, of the TKG and section 9 of the TDSV, in order to maintain network security.</p> <p>The Federal Government is to examine whether the current legislation is adequate or whether a more far-reaching obligation to retain traffic data should be created. Essentially, the actual and the legal realities have to be weighed against each other. In that equation must be included, on the one hand, secrecy of telecommunications, the basic right to informational privacy, the requirement to specify the purpose for which data is being processed, the principles of proportionality and of avoidance and economy of data, together with the basic rights of the service provider and the protection of the latter's interests, including its economic interests, and on the other hand, the legitimate interests of the security services. The Federal Government is basing its approach on guidance from the Federal Constitutional Court, which has laid down restrictive conditions for the retention of personal data for purposes other than for the original purpose of processing for official requirements or for the purpose of concluding a contract.</p>
Greece	
Ireland	<p>Directions under the Postal and Telecommunications Services Act 1983 were made by the Minister for Public Enterprise in April 2002 which require licensed</p>

Question 1: Has your country at present any special legislation concerning traffic data retention or is data traffic retention covered by existing legislation? If not are you considering legislation concerning traffic data retention?	
	<p>operators to retain existing traffic data and future traffic data for not less than 3 years after the date of their generation.</p> <p>Primary legislation is also being prepared which will require licensed operators to retain information concerning the use made of telecommunications services provided by them.</p>
Italy	<p>Italy has implemented directive 97/66/CE with law nr.171 of 13/5/1998</p> <p>Therefore, the retention of non anonymous traffic data , is not longer generally allowed. The lack of this precious information in support of criminal investigations could pose serious obstacles to the fight against criminals. For this reason there are currently more than one initiative for the review of current law.</p>
Luxembourg	
Netherlands	<p>The providers of public telecommunications networks and services are legally required to make available to the authorities the information necessary to enable them to investigate telecommunications. By this is meant monitoring or recording telecommunications and calling for traffic data (Article 13.4(1) of the Telecommunications Law). Where, however, the information required is not known to the providers, e.g. in the case of the use of pre-paid telephone cards, the providers are required to obtain and produce it. Analysis of recorded data enables number information to be obtained, the primary interest being in number information. In order to be able to obtain such information the providers are legally bound to retain certain data for a period of three months (Article 13.4(2) of the Telecommunications Law). This refers to the times when the communication took place, the numbers matching those times and the base station (Article 7 of the Decision on special recording of number information in telecommunications).</p> <p>In the Netherlands there is therefore a legal requirement to retain a certain set of data for purposes of telecommunications investigations. This requirement relates to data available to the provider in the course of running its business, which can also be analysed to obtain the number of a user who is the subject of an investigation.</p>
Portugal	
Spain	<p>Yes. Traffic data retention legislation in Spain consists of regulations on data retention for billing, marketing and customer complaint purposes, as well as Article 12 of the Information Society and Electronic Commerce Services Law (Law 34/2002 of 11 July) dealing with retention of data for national security and defence reasons and to facilitate the conduct of criminal investigations.</p> <p>The first set of rules is contained in Article 65 of the regulations approved by Royal Decree 1736/1998 of 31 July (see Spain's Official State Gazette – <i>Boletín Oficial del Estado</i> – of 5 September 1998) implementing Title III of the General Telecommunications Law in relation to the universal telecommunications service, all other public service obligations and the public obligations of providers of telecommunications services and operators of telecommunications networks. Article 65 establishes a general obligation to destroy personal traffic data upon termination of the communication except in the case of:</p> <ul style="list-style-type: none"> – Data processed for interconnection billing and payment purposes. – Data stored for billing purposes for the period during which invoices can be contested or payment demanded. – Data processed for the purpose of marketing the communications services

Question 1: Has your country at present any special legislation concerning traffic data retention or is data traffic retention covered by existing legislation? If not are you considering legislation concerning traffic data retention?

offered by the operator concerned, subject to the subscriber's consent.

Article 12 of the Information Society and Electronic Commerce Services Law (Official State Gazette of 12 July 2002) requires traffic data to be retained for use in connection with criminal investigations and for safeguarding public security and national defence. This obligation is confined to communications generated during the provision of information society services and the rules governing it are in accordance with the conditions laid down in Article 15(1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Article 12 of Law 34/2002 is transcribed below in its entirety.

"Article 12. Duty to retain traffic data relating to electronic communications

1. Operators of electronic communications networks and services, providers of access to telecommunications networks and host service providers shall retain connection and traffic data generated by communications established during the provision of an information society service for a maximum period of twelve months in the manner required by this Article and its implementing rules.

2. The data retained by operators of electronic communications networks and services and providers of access to telecommunications networks in compliance with the preceding paragraph shall be solely those necessary to facilitate the localisation of the terminal employed by the user to transmit the information. Host service providers shall retain only such data as are essential to identify the source of the stored data and the time when the provision of the service commenced.

In no case shall the obligation to retain data affect the confidentiality of communications.

The operators of electronic communications networks and services and the service providers referred to in this Article shall not use retained data for purposes other than those indicated in the following paragraph or permitted elsewhere under this Law, and they shall adopt appropriate security measures to prevent the loss or alteration of such data and unauthorised access thereto.

3. Data shall be retained for use in connection with a criminal investigation or to safeguard public security and national defence, and shall be made available on request to judges, courts or the State Prosecutor's Office. The communication of such data to the law enforcement agencies shall be subject to the legislation on personal data protection.

4. The categories of data to be retained based on the type of service provided, the period during which such data are to be retained in each case, subject to the maximum period provided for in this Article, the conditions under which they are to be stored, processed and held in safekeeping, the form in which they are to be delivered to the bodies authorised to request them and the manner in which they are to be destroyed upon expiry of the relevant retention period unless they should be required for these or other purposes provided for in this Law, shall be as defined in the relevant implementing regulations."

The application of the foregoing provisions will require a Regulation setting out specific rules for the various aspects of data retention referred to.

Sweden

Swedish telecommunications legislation gives operators certain possibilities to retain traffic data without consent from the subscriber. This applies to information necessary for billing of subscribers and payment for certain other

<p>Question 1: Has your country at present any special legislation concerning traffic data retention or is data traffic retention covered by existing legislation? If not are you considering legislation concerning traffic data retention?</p>	
	<p>charges. Information can also be saved in so far as it is necessary to uncover unauthorised use of the network.</p> <p>A Government Committee has given consideration i.a. to parts of the new Data Protection Directive, in a recently published report in which new telecommunications legislation is proposed. Although article 15 of the Directive provides a possibility to instruct operators to retain traffic data to meet needs of law enforcement authorities, no such obligation is suggested in the report. This issue is, however, presently the subject of discussions in Sweden.</p>
<p>United Kingdom</p>	<p>In the UK the Anti-Terrorism Crime and Security Act was passed in 2001, an emergency piece of legislation, in response to the attacks on the USA on September 11 of last year. Part 11 of that Act specifically deals with the retention of communications data for the following purposes:-</p> <ul style="list-style-type: none"> i. for the purpose of safeguarding national security; or ii. for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security. <p>The Act outlines the requirement for, at least initially, a voluntary Code of Practice relating to data retention. This voluntary Code or Practice is currently under development. The Home Office is in the process of consulting with industry, the Office Information Commissioner, other government departments and law enforcement agencies.</p>

Questionnaire 2: Has your country yet focussed on a specific period of time for the retention of traffic data? Have you also considered what kind of traffic data should be retained?	
Country	Answer
Austria	The current obligation to retain data for subscriber billing applies up to the deadline for legally contesting the bill or asserting a claim to payment. Moreover, exchange data must immediately be erased or made anonymous by the service provider when the call is terminated (see also reply to Question 1; Section 93(1) and (2) of the TKG).
Belgium	The Computer Crime Act provides that the period for the retention of data will be determined in the implementing regulation to be taken by the government; however, it is already specified that this period shall be of a minimum of 12 months. The type of data to be retained shall also be determined in the implementing regulation. These data are broadly defined in the Computer Crime Act as data related to the "call" ("données d'appel" in French) via means of telecommunications and data related to the identification of the user of telecommunication means. The implementing regulation is under preparation; at this stage, this preparation has not yet given rise to a public text.
Denmark	As it appears from the answer to question 1 above, telecommunications companies and Internet service providers according to section 786 of the Administration of Justice Act have to record and store ("log") the information on tele communications and Internet communications for one year. The detailed (technical) rules on this logging – including regulation on what kind of traffic data must be recorded and stored – will be prescribed by the Minister of Justice following negotiations with the Minister of Science, Technology and Innovation and otherwise following a dialogue with the industry.
Finland	According to the Act on the Protection of Privacy and Data Security in Telecommunications, section 10.2 a telecommunications operator may process identification information relating to the determination of the telecommunications bill for a maximum period of three years after the telecommunications bill has been paid in full, however, not longer than the payment of the telecommunications bill may be collected unless otherwise provided for elsewhere. The obligation of a telecommunications operator to store identification information relating to the determination of a telecommunications bill shall be provided for by Decree. According to the above mentioned Decree on the Protection of Privacy and Data Security in Telecommunications the operator is obliged to store identification information relating to the determination of a telecommunications bill at least 3 months from the date the bill has been due. If there is a disagreement concerning the telecommunications bill, the information has to be kept until the matter has been agreed upon or solved. The police authorities and Ministry of Interior has considered that the appropriate and effective time for the operators to keep the traffic data (including connection information, "logs") should be 2 years. This should be taken into account when updating the Privacy Protection Act.
France	
Germany	The comments on question 1 refer to the existing situation under German law with regard to the possibility of data retention. The question of the period of time

Questionnaire 2: Has your country yet focussed on a specific period of time for the retention of traffic data? Have you also considered what kind of traffic data should be retained?	
	for retaining data will be examined in connection with a possible data-retention obligation.
Greece	
Ireland	<p>The Direction (referred to in Answer 1) requires licensed operators to retain existing traffic data and future traffic data for not less than 3 years after the date of their generation.</p> <p>The proposed primary legislation (referred to in Answer 1) will require licensed operators to retain information concerning the use made of telecommunications services provided by them for any person for a period of 3 years after such use. It is expected that traffic data in the primary legislation will be defined in same manner as it has been in the Directions. Traffic data will mean any data processed by the licensed operator in connection with transmitting or receiving a telecommunication message on a telecommunications network or charging for it and includes, in relation to any message, data concerning</p> <ul style="list-style-type: none"> (a) its routing, duration or time, (b) the location of the sender's or recipient's terminal equipment, (c) the network on which the message originates or terminates, and (d) the beginning, end or duration of its connection to the network.
Italy	<p>It is quite difficult to be aware in advance of how much time it will take from the moment the crime was committed and the beginning of the investigation. Therefore, as a general principle, the longer traffic data is retained the better it is. However we do understand that the retention of this information for an unlimited period is not possible. The general understanding is that high tech investigation very rarely start a year later the incident has occurred. It should be also considered that traffic data are both saved on-line and off-line (on storage media). Data on-line are easily available but the storage available space is limited. Off-line data are saved on storage media, are generally not immediately available, but can be stored on a practically unlimited space. Some providers make a precise distinction between on-line and off-line preservation time. For what concerns the kind of data that should be retained by Internet Service Provider, Italy, together with other G8 members, assembled a specific list (attached) of minimum data that should be preserved for law enforcements needs.</p>
Luxembourg	
Netherlands	As stated above, there is a legal requirement in certain specific cases to retain a limited set of data for a period of three months after the data have been processed for the first time. This requirement is limited to the times when the communication took place, the numbers matching those times and the base station.
Portugal	
Spain	<p>Period of retention:</p> <p>No specific time period is stipulated in relation to the retention of data provided for in Article 65 of the Regulation approved by Royal Decree 1736/1998 of 31 July, with the length of time for which the traffic data may be retained varying depending on the purpose for which the data are used. Accordingly, the maximum periods are as follows:</p> <ul style="list-style-type: none"> - Billing: as long as necessary. - Dealing with customer complaints: five years (general limitation period for

Questionnaire 2: Has your country yet focussed on a specific period of time for the retention of traffic data? Have you also considered what kind of traffic data should be retained?

personal actions).

- Marketing: indefinite (the data may be used until the customer withdraws his consent).

A maximum period of 12 months has been established in relation to the retention obligation provided for in Article 12 of Law 34/2002. This maximum period will be stipulated in each case by the Regulation implementing Article 12.

Type of data:
Article 65 of the Regulation approved by Royal Decree 1736/1998 sets out the data which can be retained for the purposes of billing, dealing with complaints and marketing:

- The number or identity of the customer.
- The address of the customer and the type of terminal used for the calls.
- The number of units to be billed during the accounting year.
- The number of the customer who receives the call.
- The type, time of commencement and duration of the calls made or the volume of data transmitted.
- The date of the call or service.
- Other data relating to payments, such as payment in advance, payment in instalments, disconnection and notification of bills.

Pursuant to Article 12 of Law 34/2002, the data which must be retained are "connection and traffic data generated by communications established during the provision of an information society service". Article 12 stipulates that this refers only to the data necessary to:

- Facilitate the localisation of the terminal employed by the user to transmit information, in the case of data to be retained by Internet access providers and telecommunications operators.
- Identify the source of the data stored and the time at which provision of the service commenced, in the case of data to be retained by host service providers.

In no circumstances may the data retained include data protected by the confidentiality of communications.

Sweden The Committee report suggests that that traffic data may be retained no longer than 12 months. Law enforcement authorities have suggested that a minimum of 12 months is necessary. Discussion on what kind of traffic data should be retained is only in its initial stages.

United Kingdom Currently the time periods under consideration vary according to the type of data concerned they are a minimum of 6 months and a maximum of 12 months for retained data.

Communications data has been defined in the following way:-
"Communications data" means any of the following-

- a. any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunications system by means of which it is being or may be transmitted;
- b. any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person –
 - (i) of any postal service or telecommunications service; or
 - (ii) in connection with the provision to or use by any person of any

Questionnaire 2: Has your country yet focussed on a specific period of time for the retention of traffic data? Have you also considered what kind of traffic data should be retained?

- telecommunications service, of any part of a telecommunication system;
- c. any information not falling within paragraph (a) and (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.
- (1) **Traffic data** in relation to any communication, means-
- (a) any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted,
- (b) any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted,
- (c) any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and
- (d) any data identifying the data or other data as data comprised in or attached to a particular communication,
- but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.
- "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

Questionnaire 3: Has your country considered allowing traffic data retention for purposes other than billing, such as network security purposes?	
Country	Answer
Austria	The Austrian Federal Ministry of Transport, Innovation and Technology is currently preparing a Law on Communications, which already exists in draft form. Consideration is being given to inclusion in the draft of a rule obliging providers to retain exchange data for a given period for prosecution purposes.
Belgium	Compulsory data retention under the Computer Crime Act is only provided in the framework of criminal investigation. There is no legal initiative presently pending regarding data retention dedicated to secure networks.
Denmark	The amendment of section 786 of the Administration of Justice Act was as mentioned above passed by Parliament in order to improve the investigative possibilities of the police.
Finland	Yes. According to the Act on the Protection of Privacy and Data Security in Telecommunications, section 18, the police has a right to obtain information about calls made to a subscription when it is necessary for the investigation of certain serious crimes as well as the identification information relating to messages sent from a mobile phone. In addition to that the operator may give police or other authorities receiving emergency calls the necessary identification information, such as the number, installation address, user, location of the support station through which the emergency call has been placed. The right of an authority to obtain identification information for the pre-trial investigation shall be governed by the Coercive Measures Act (450/1987).
France	
Germany	See reply to question 1.
Greece	
Ireland	The proposed primary legislation on the retention of traffic data will provide for compliance with any request from the police (Garda Síochána) or the Defence Forces for disclosure of data, in the interests of the prevention and investigation of serious crime, in the interests of national security and in the discharge by Ireland of its international obligations relating to terrorism.
Italy	Yes, as said before, the limiting of data retention only for billing purposes does not take into right consideration the need for both private and public safety. The review of current legislation should include also cover these important issues.
Luxembourg	
Netherlands	Yes. Within the context of discussions on the new privacy directive for the electronic communications sector, the Netherlands has urged to have explicit provision for the option in Article 6 of the directive, whereby traffic data may be used in non-anonymous form not only for billing but also for prevention of fraud, traffic regulation and the provision of information to customers. This proposal has been rejected by the other Member States and by the Commission.
Portugal	
Spain	Yes, for the purposes referred to in Article 12.3 of Law 34/2002.
Sweden	According to present legislation, traffic data need not be erased or made anonymous so far as it is necessary to prevent or uncover unauthorized use of the network. New rules in this regard are not considered at present.
United	Under the Anti-terrorism, Crime and Security Act 2001 data can be retained for

Questionnaire 3: Has your country considered allowing traffic data retention for purposes other than billing, such as network security purposes?

Kingdom	two purposes over and above business purposes. These are:- for the purpose of safeguarding national security; or ii for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security. The telecommunications industry is able to retain data for business purposes and where appropriate this may include purposes such as network security.
---------	--

Questionnaire 4: What is the present procedure for a law enforcement authority to obtain traffic data from a service provider? Has this procedure proven to be efficient and effective?

Country	Answer
Austria	<p>Under Section 89(2) of the TKG, service providers are obliged to cooperate to the necessary extent in surveillance of telecommunications; they are obliged to make available all equipment needed for surveillance of a telecommunication by Section 89(1) of the TKG. Such obligation is given concrete form in Section 3(2) of the Order of the Federal Minister for Transport, Innovation and Technology concerning the surveillance of telecommunications (Surveillance Regulation – ÜVO). Pursuant thereto, most telephone-service providers must have ready in their installations the facilities for making available content and any other information necessary for the surveillance of telecommunications; this means above all: the address of the subscriber line under surveillance, the addresses dialled from the subscriber line under surveillance, even when a call does not get through, any incomplete addresses dialled from the subscriber line under surveillance, where an attempted call is prematurely terminated, the addresses of subscriber lines from which the subscriber line under surveillance is dialled, even when a call does not get through, in the case of mobile-telephone lines under surveillance, the cells carrying the call under surveillance, the beginning of the call or attempted call with date and time, the end of the call or attempted call with date and time and the duration of the call. Straight internet-service providers are not covered by the obligations in the Surveillance Regulation (ÜVO). Both content and exchange data are released to prosecuting authorities by the service provider solely on the basis of a court decision pursuant to the Code of Criminal Procedure (Sections 149a et seqq of the StPO). As from 1 October 2002, where providers are obliged to cooperate (Section 89(2) of the TKG), they must in addition be instructed as to the scope of that obligation by court decision. On the basis of a court decision, providers are obliged to release exchange data. This is done by providers' employees examining the relevant data and communicating them to the court or to the Police or Gendarmerie Department responsible for the investigation.</p>
Belgium	<p>The present procedure is the procedure which allows the tracking or the interception of telecommunications. Police officers cannot autonomously ask an ISP (Internet Service Providers) for traffic data. Public Prosecutors can autonomously issue a request to obtain traffic data from an ISP. In most cases these requests have to be confirmed by an Examining Magistrate. Interception of traffic data is only allowed for the purpose of the investigation of a limited number of serious crime.</p> <p>The request has to be motivated (mention facts and legal provisions). The request can ask for historical data but also for traffic data of future connections. In most cases the execution of the formal request of the magistrate is done by a police officer.</p> <p>The present procedure enables to have access to traffic data, but only if these data are retained by the ISP. Privacy regulation, including Community Law, considerably limit the type of data which can be retained and the period during which the retention is allowed. Most of the time, traffic data will therefore not be available any more when the law enforcement authorities need to have access to them.</p>
Denmark	Chapter 71 of the Danish Administration of Justice Act contains rules on

Questionnaire 4: What is the present procedure for a law enforcement authority to obtain traffic data from a service provider? Has this procedure proven to be efficient and effective?

	<p>invasion of the secrecy of communication, observation and data capture. According to Section 780, paragraph 1, number 3, the police pursuant to rules of this chapter can invade the secrecy of communication by inter alia obtaining information about which telephones or other similar communication devices are connected with a certain telephone or other communication device, even though the owner thereof has not yet granted permission hereto (tele-information). The police can also invade the secrecy of communication according to section 780, paragraph 1, number 4, by obtaining information about which telephones or other similar communication devices within a certain area are connected to other telephones or communication devices (extended tele-information). In principal invasion of the secrecy of communication can only take place after a court order, but the police may, in cases where the purpose will be forfeited if a court order has to be awaited, order the invasion of the secrecy of communication without a court order. In these cases the police are obligated to present the case before the court as soon as possible and at latest within 24 hours. The rule concerning logging does as mentioned above not involve extended police access to traffic data.</p>
Finland	<p>For the telecommunications monitoring permits the official with the power of arrest has to present a written request to the court that makes the decision. The hearing on such a request shall take place without delay and in the presence of the requesting official or another official assigned by him (Coercive Measures Act, chapter 5a, sections 3, 5 and 6). Telecommunications interception and telecommunications monitoring has proven to be very effective. Telecommunications monitoring has been crucial or very important for criminal investigation in 65 per cent of the cases where the monitoring permit has been granted. In cases covered by the Privacy Protection Act statistics are not collected.</p>
France	
Germany	<p>Sections 100g and 100h of the Code of Criminal Procedure (StPO) govern the right of the criminal prosecution authorities to obtain disclosure of telecommunications traffic data. They allow the police and public prosecutors to seek disclosure of telecommunications traffic data by those who provide telecommunications services on a commercial basis, or who play a part therein, in cases where it is suspected that a person has committed, or participated in committing, a serious criminal act or has attempted to do so in cases where such attempt is also an offence. In cases where it is suspected that a criminal act has been committed using telecommunications transmission equipment such as a computer, disclosure of traffic data may also be sought in the case of a less serious criminal act, since it would otherwise be virtually impossible to solve such crimes. The supply of telecommunications services on a commercial basis involves the sustained provision of telecommunications, including the provision of transmission channels for third parties, with or without the intention of making a profit. Thus, in addition to telecommunications undertakings, including Internet service providers, operators of corporate networks also have an obligation to disclose data. Extension equipment, for example in hotels, hospitals, factories and offices, may also be covered. The right of the criminal prosecution authorities to obtain disclosure applies to</p>

Questionnaire 4: What is the present procedure for a law enforcement authority to obtain traffic data from a service provider? Has this procedure proven to be efficient and effective?

	<p>both past – in relation to the time of the order – and future telecommunications traffic. Disclosure may only be sought where the traffic data concern the accused or so-called communication mediators, i.e. persons of whom it may be assumed, by reason of certain facts, that they receive – even in good faith – (e.g. the victim of a hacker) or pass on, a communication intended for the accused or originating from him or that their connection is used by the accused.</p> <p>The right to disclosure of the criminal prosecution authorities does not, however, provide the basis for any obligation to retain data. The provisions of sections 100g and 100h of the StPO are in fact based largely on the data-protection rules in the TKG concerning the retention of personal data.</p> <p>The disclosure order must contain the name and address of the targeted individual and the call number or other call sign of his telecommunications connection (section 100h, paragraph 1, first sentence, StPO).</p> <p>Disclosure of telecommunications data has to be ordered by a judge. When delay would be prejudicial, the Public Prosecutor's Office may issue the order. The order issued by the Public Prosecutor's Office expires unless it is confirmed within three days by a judge (Section 100h(1), third sentence, StPO). It is not permissible for the police to issue an order.</p> <p>The order has to be issued in writing. Where it relates to disclosure of future telecommunications data, it may be valid for a maximum of three months, with the possibility of extension for additional maximum periods of three months at a time if the conditions which led to it being issued continue to exist (Section 100h (1), third sentence, StPO).</p> <p>The persons concerned, i.e. in particular those who are the subject of the order, are to be notified that information is being disclosed as soon as this can be done without endangering the purpose of the investigation, public security, or human life or limb, or the possible continued use of an undercover police officer (Section 101(1), first sentence, StPO).</p> <p>Sections 100g and 100h StPO did not enter into force until 1 January 2002. The Federal Government does not yet have any information based on practical experience with the new provisions.</p>
Greece	
Ireland	<p>There is a provision in law for the disclosure to the police (Garda Síochána) and the Defence Forces by licensed operators providing telecommunications services of information concerning the use made by any person of those services (the Postal and Telecommunications Act 1983, as amended by the Interception of Postal Packets and Telecommunication Messages (Regulations) Act 1993). This provision requires that such a request should be submitted in writing by a chief superintendent of the police (Garda Síochána) or a colonel of the Defence Forces. Yes.</p>
Italy	<p>Traffic data are handled to law enforcement exclusively on the basis of a judicial order (exhibition decree). The procedure causes not particular problems although is obviously limited to the Italian territory.</p> <p>Ministry of Justice:</p> <p>In a criminal investigation, it is possible to obtain telecommunications data (telephone numbers concerned and relevant holders, records of conversations made in a given period of time) by means of an order issued by a judge or a public prosecutor prescribing the presentation or seizure of the available records.</p>

Questionnaire 4: What is the present procedure for a law enforcement authority to obtain traffic data from a service provider? Has this procedure proven to be efficient and effective?	
	<p>Said order is enforced by the judicial police in the premises of the telecommunications company concerned.</p> <p>Under Italian law, in criminal proceedings communications at a distance or taking place at the presence of the persons involved can be wiretapped on the basis of an order issued by a Pre-trial Investigation Judge upon request of a public prosecutor. In urgent cases, said order can even be issued by a public prosecutor and subsequently validated by a Pre-trial Investigation Judge.</p> <p>Legislation in force has so far ensured efficient and effective data acquisition as well as wiretapping and indoor listening.</p>
Luxembourg	
Netherlands	<p>The public prosecutor has the authority to require, in connection with a criminal investigation (Article 126n Code of criminal procedure), that information be provided regarding all traffic which has taken place via the telecommunications infrastructure or via a telecommunications installation used in providing a service to the public, and regarding which there is reason to believe that the suspect has been involved. The provider is required to satisfy any such requirement. In practice, this is referred to as "printer lists" or "printer taps".</p> <p>There have been no complaints hitherto about the application of this procedure.</p>
Portugal	
Spain	<p>Data may only be retained with judicial authorisation, at the request of the public prosecutor's office or the police authorities, in the course of criminal investigations in general.</p> <p>The current procedure is not completely satisfactory for the purposes of avoiding the destruction or loss of the data being investigated, which demonstrates the need for immediate (pending judicial authorisation) retention measures which are not dependent on the willingness of the service providers.</p>
Sweden	<p>Law enforcement police authorities can request the release of such data from a service provider, in a specific case of investigating a crime that could lead to imprisonment in no less than two years. This procedure has by and large worked well.</p>
United Kingdom	<p>The present procedure is outlined in a comprehensive document jointly published by the Association of Chief Police Officers and HM Customs and Excise. This Manual of Standards for Accessing Communications Data describes accepted routes of obtaining such data and the appropriate legislation prescribed for the purpose.</p> <p>The process has been as efficient as the limited resources of the CSP units has allowed - the problem has been the legal position. Access under the DPA has been considered to be not 'by law' as required under HRA. LE and Industry have reasonable working agreements that cover the acquisition of Communications data</p>

Questionnaire 5: Have you received any reports from your law enforcement authorities that have indicated an obstruction of their work due to the non-existence of appropriate legal instruments concerning traffic data retention?

Country	Answer
Austria	<p>Until the Surveillance Regulation (ÜVO) entered into force, there were continually problems with service providers concerning the extent of their obligation to cooperate. Now there are occasional differences of opinion about the classification of certain data (e.g. IMEI numbers). Since telecommunication-service providers, and in particular internet providers, are increasingly making use of flat-rate billing or providing their services free of charge, storage of traffic data is not in such cases necessary for billing and not therefore permitted. This could in future lead to insufficient availability of traffic data even for prosecution purposes.</p>
Belgium	<p>Yes, police authorities have indicated that there is a lack of efficiency in the existing procedure since it does not ensure that traffic data have to be retained, and therefore does not ensure that these data will be available, if necessary, for the purpose of the investigation: see the last paragraph of the previous answer. Traffic data are very important for the investigation of computer related crime : access to these data allow investigators to make the chain from the destination of a communication to the origin of it or vice versa. This implies that each provider in the chain that was used to establish the communication from physical level to the application or service level, has to retain the link to the previous and next provider in his logged traffic data.</p> <p>Furthermore, police authorities have identified the following problems related to traffic data which already complicate the use of these data in the course of criminal investigation. Given these difficulties and the importance of traffic data for the investigation of computer related crime, it is therefore essential to extend the opportunities to retain traffic data.</p> <p>Practical problems exist</p> <p>Although they offer access or services in Belgium, some Internet Access Providers (IAP) or Internet Service Providers (ISP) try to evade legal obligations to retain traffic data by installing their technical infrastructure in a geographical region where there are no such strict legal obligations or where there is another legal framework. Belgian LE officers can in these cases not enforce their legal powers to obtain traffic data. It is in these cases for Belgian LE also impossible to verify if legal obligations of IAP or ISP concerning data privacy are applied.</p> <p>The anonymous use of Internet connections in cyber cafés or libraries causes very often problems. In most cases there are no log files stored and the users are not obliged to identify them selves.</p> <p>Private companies that offer Internet connections to their employees (sometimes several hundreds) are in most cases not obliged to retain traffic data, which makes it difficult to continue investigations inside these companies.</p> <p>Free Internet access accounts offered by IAP's do not require any verifiable identification. If these providers do not log the CLI or any other identification on the physical link level (like modem serial numbers or MAC addresses) it is not possible to identify the source of the communication.</p> <p>Virtual ISP's depend on a contracted Internet service provider to give Internet access to their customers. There is often no link between the IP-address (that is given by the contracted firm) and the subscriber information (that is retained only with the virtual ISP).</p>

Questionnaire 5: Have you received any reports from your law enforcement authorities that have indicated an obstruction of their work due to the non-existence of appropriate legal instruments concerning traffic data retention?

It is **sometimes impossible** for the IAP to register the link to the underlying level because it is not provided. E.g. if the **CLI is blocked**, they cannot register that information which is crucial in the chain to the origin of the communication. Several Internet access providers oblige their customers to pass over their **proxy-servers**, an **intermediate system** that is used to save bandwidth. These IAP do not log or retain data of the proxy-server activity for a long period. The address that is logged at the ISP, is that of the proxy-server of the IAP and not that of the original Internet user. If no proxy-server logs are retained, in most cases it becomes impossible to identify the end user.

A solution proposed by the Internet service providers using these kinds of proxy-servers, is to send the IP-address of the origin of the request to the service provider on the Internet.

This offers of course no solution if the service provider is not obliged to retain that information.

Anonymizers are systems similar to proxy servers but are especially set up to render the technical identification of the source of the communication impossible. These anonymizers are often systems set up by cyber-criminals.

Not all system clocks of Internet access and service providers are **synchronised** with the correct "legal time" which makes the interpretation of the traffic data in the log files difficult, especially if this data has to be compared with data in log files from other IAP or ISP.

Inaccurate time stamps in log files can prevent the investigators to find the suspects and could lead to the wrong indication of innocent users as a suspect. Sometimes a **combination of** more of the above mentioned **problems** that make it impossible for investigators to continue their investigations.

Future problems : Although this system is not yet widely used in Belgium, we can foresee in the near future Internet connections offered through **wireless connections (WIFI)** by all kinds of firms that install access points. Depending on the way of how users will be identified, this way of offering Internet access can cause **similar problems as we now encounter in cyber cafés**. As the radius of action of these access points often goes beyond the building walls, one will be able to connect without even entering the building in which the access point is installed, making identification even more difficult.

Denmark

The amendment of section 786 of the Administration of Justice Act was as mentioned above passed by Parliament in order to improve the investigative possibilities of the police. It was the general apprehension of the law enforcement authorities that the telecommunications industry to a large extent could not be expected to store traffic data in the future, due to the fact that the retention of traffic data increasingly can not be justified for billing purposes (flat rate subscription etc.).

On the basis of police experiences when investigating criminal offences that involve the use of modern technology, it was considered necessary in order to improve the investigative possibilities of the police to ensure the recording and storing of traffic data that the police might be in need of when investigating (notably serious) criminal offences.

Finland

Lack of obligation to retain data traffic has occasionally been a hindrance at criminal investigations.

At the moment there are some difficulties in receiving traffic data, since the

Questionnaire 5: Have you received any reports from your law enforcement authorities that have indicated an obstruction of their work due to the non-existence of appropriate legal instruments concerning traffic data retention?

	<p>operators interpret the Privacy Protection Act in the way that they can give out traffic data only in the cases stated in the Privacy Protection Act (section 18) or with a telecommunications monitoring permit. Therefore there is a so called "grey area" in between the provisions, where the rules of conduct are some what unclear or they are missing altogether. For example investigation on alleged libel on the internet often seize for the fact that traffic data is not handed out. There are several other crimes that are not included in the list in the Privacy Protection Act nor do they fulfil the requirements to ensure telecommunication monitoring permit.</p> <p>By large, in the connection with crimes on information network, the biggest problems are international contacts. Receiving information from other member states or especially from third countries is very difficult. The information gets frozen in EU to a server when requested, but to pull through the official procedure on it, according to long time experience, it takes months, even years. From third countries it is practically impossible to get information ever.</p> <p>There is a Government Proposal being discussed in parliament for the renewal of the Coercive Measures Act. In the proposal in Chapter 5a, section 3 will be included, in addition to monitoring telecommunications connection the authorities will be able to get a monitoring permit also for IP-addresses. However, this does not remove the problem that investigation of some crimes is still not covered by a possibility of acquiring traffic information (see above).</p>
France	
Germany	Yes, there have been reports from German law enforcement agencies to the effect that the provisions in force in Germany are not sufficient for the purposes of their work. They call for service providers to be required to retain data beyond a limited period of time.
Greece	
Ireland	No.
Italy	<p>Even if only a few cases were reported, the lack of appropriate legislation on data retention might become a critical issue in an ongoing investigation.</p> <p>Ministry of Justice: No.</p>
Luxembourg	
Netherlands	One of the priorities identified in the national action plan on counterterrorism and security was the conduct of an investigation into the categories of data retained by telecommunications providers and the obstacles experienced by the criminal investigation and intelligence and security services because of the absence of an obligation to retain historical traffic data. The investigation is being carried out at the moment and is expected to last until the end of the year. The results will determine whether there is a need to introduce additional obligations to retain data. Article 8 of the ECHR must be taken into account in this context.
Portugal	
Spain	Yes.
Sweden	As indicated under 4., present national procedures work well.
United Kingdom	Yes I have received reports of LE agencies expressing frustration that Data that could further a criminal investigation has been destroyed. This destruction had

Questionnaire 5: Have you received any reports from your law enforcement authorities that have indicated an obstruction of their work due to the non-existence of appropriate legal instruments concerning traffic data retention?

been in line with the companies data retention policies, in some cases, despite the fact that agencies had received copies from which evidence had been prepared. Yes had there been a legal policy of mandatory or voluntary detention then this data may have been made available.

Questionnaire 6: Have you entered into a permanent dialogue with your telecommunications industry about the issue of traffic data retention and what are the tendencies you have observed? How would you judge the general willingness of the telecommunications industry operating in your country to embark on a retention of traffic data?	
Country	Answer
Austria	The Austrian Ministry of Justice has only recently sounded out in conversation the views of representatives of the service providers operating in Austria concerning the possibility of an obligation to retain exchange data. There was clearly a basic <i>readiness on the part of providers to agree</i> to the introduction of such an obligation.
Belgium	A more formal dialogue with the industry should take place during the drafting of the secondary legislation which will implement the principle set up in the primary legislation. However, the first contacts have shown a fairly high willingness of the telecommunications industry for co-operation in this field. An harmonised system for the European Union would be an important factor for obtaining the support of the industry.
Denmark	Before the Parliament's passing of the amendment of section 786 in the Administration of Justice Act, the bill on this matter was submitted to the telecommunications industry, and the telecommunications industry obtained an interview with the Danish Parliament. In addition to this the detailed (technical) rules on this logging will be prescribed following a dialogue with the telecommunications industry.
Finland	Discussions with telecommunication industries have been started in connection with the implementation of the directive concerning Protection of Privacy and Data Security in Telecommunications. The telecommunications industry is rather reluctant in retaining traffic data for any other than business related purposes. The operators do not collect or store any information for the authorities. All the information that is available for the authorities is information that operators use and store for billing purposes.
France	
Germany	The departments concerned – the Federal Ministry of Justice, the Federal Ministry of Economic Affairs and Technology and its subordinate authority, the Regulatory Authority for Post and Telecommunications (RegTP), and the Federal Ministry of the Interior and its subordinate authority, the Federal Bureau of Criminal Investigation – maintain contacts with telecommunications and data communication associations and enterprises. On economic grounds and for reasons of data protection, the associations and service providers tend to be critical of any obligation to retain traffic data. In particular, they are afraid of being at a competitive disadvantage vis-à-vis foreign service providers and having to pay high costs for storing data.
Greece	
Ireland	No - The telecommunications industry operators have, to date, facilitated the obtaining of call-related data for the purposes of the investigation of serious crime or national security and we do not foresee problems arising with the industry in relation to the primary legislation referred to at 1 above.
Italy	In Italy it was set up a dedicated inter ministerial working group (Communications, Justice and Interior) composed by experts. One of the team's goal is identify specific services that telecom providers will be compelled to offer

Questionnaire 6: Have you entered into a permanent dialogue with your telecommunications industry about the issue of traffic data retention and what are the tendencies you have observed? How would you judge the general willingness of the telecommunications industry operating in your country to embark on a retention of traffic data?

	<p>to investigators. At the same time the group is also trying to quantify the cost of each of these services that government will pay to the telecom provider. The problem of the cost was in fact one of the obstacles claimed by service providers to the retention of data. The whole process of identify services and costs is in progress in very close cooperation with the major Italian providers' associations. Dialogue between telecommunications industry and government was a concept endorsed by the G8 Justice and Interior ministers at their last summit.</p> <p>Ministry of Justice: Neither the Ministry of Justice nor judicial authorities have permanent relations with telecommunications companies in respect of keeping telecommunications data.</p>
Luxembourg	
Netherlands	<p>Yes, there is a permanent consultation structure, the "Post and Telecommunications Consultation Body" (OPT). The "Interception Body" (DAF) is a component of the consultation structure. Consultations in the DAF involve representatives of the various telecommunications providers active on the Netherlands market and representatives of the government bodies concerned (Ministries of the Interior, Economic Affairs and Justice, the Public Prosecutor's Office and the police).</p> <p>In general, the willingness of the telecommunications industry to retain traffic data cannot be judged as entirely positive. Providers are reticent on this point because of the business aspects and possible damage to their image. Retaining traffic data, which cannot be used by the providers themselves, involves costs. Another consideration is the importance of protecting the privacy of telecommunications industry clients.</p>
Portugal	
Spain	<p>The Spanish authorities have held and continue to hold discussions with companies and users affected by the legislation on the retention of personal data. With respect to the tendencies observed, it has been established that information society service providers retain some traffic data for billing operations and for security reasons (detection of e-mail accounts from which junk mail or computer viruses are sent).</p> <p>As regards their attitude to complying with the obligation to retain data provided for in Article 12 of Law 34/2002, although they are not familiar with the details of the measure (the implementing Regulation for that Article has not yet been issued), information society service providers have expressed their concern regarding the possible cost of storing and processing such data. In this respect, they have requested the introduction of some form of economic or tax-related compensation to offset any extraordinary costs resulting from compliance with the obligation.</p> <p>In this connection, they also considered that an over-costly obligation could constitute a barrier to entry into the market for the smaller service providers and an obstacle to the free provision of services in the Community if the regulations were more restrictive than those established in other Member States.</p> <p>Therefore, although companies in the industry are willing to cooperate with the authorities in the exercise of their functions, they are opposed to measures that</p>

Questionnaire 6: Have you entered into a permanent dialogue with your telecommunications industry about the issue of traffic data retention and what are the tendencies you have observed? How would you judge the general willingness of the telecommunications industry operating in your country to embark on a retention of traffic data?

	entail extra costs for their activity.
Sweden	Representatives of industry are consulted when new legislation in the telecommunications sector is considered. We are not in a position to judge the opinion of the whole industry concerned. Some service providers do, however, already retain traffic data for varying periods, i.a. for their own efforts to fight unauthorised use of the networks. The Committee report on new legislation is currently in a consultation process with i.a. representatives of industry. When that process is concluded, we will have a fuller picture of the views of the industry.
United Kingdom	Yes the UK does have permanent dialogue with the industry. The initial response was for "voluntary" arrangements to be made during the "Bill" stage of the Anti-terrorism Act. However industry now appear to be of the opinion that a mandatory system would provide the correct level of protection from corporate liability litigation. The industry are willing to work with the government on the issue of data retention and the efforts made by them in the attempts to deliver a "voluntary" code have given a clear indication of their level of support for such action.

Questionnaire 7: How would you rate the solution of creating an instrument on traffic data retention for law enforcement purposes at a European level?	
Country	Answer
Austria	The Austrian Ministry of Justice and the Austrian Ministry of the Interior would welcome a binding rule (possibly in the form of a framework decision) on retaining exchange data for prosecution purposes subject to the principles of proportionality. The Federal Chancellery, which is chiefly responsible for data-protection concerns, is sceptical about such a rule.
Belgium	Given the growing importance of computer related crime and the transnational dimension of that form of criminality, it is essential to have common policies developed at the European level. Data retention being a useful tool for investigating cybercrime, as well as serious crime involving the use of a computer, the general principles of data retention should be determined in an EU instrument. This EU instrument could be a framework decision harmonising not only the obligation of data retention but also basic procedural safeguards. Having procedural safeguards mentioned and defined in the framework decision should soften the debate and show that the orientation of EU criminal law is not only repressive, which is unfortunately more and more argued among the civil society. Elaborating an EU instrument on data retention for the purpose of criminal investigation will require a deep analysis but, given the results obtained in JHA matters of a similar importance, one needs to be confident in the ability of the Council to achieve this task. Belgium is presently contemplating a proposal in this sense.
Denmark	As it appears from the above mentioned, the insertion of a new provision into section 786 of the Administration of Justice Act concerning the recording and storing of traffic data ("logging") was considered to be a necessary amendment in order to ensure the retention of traffic data for law enforcement purposes. When investigating serious crimes, the possibility of invading the secrecy of telecommunication is an important and efficient investigative tool for the police. Due to the changes in the varieties of the subscriptions of telecommunication this investigative tool was considered in risk of being of no use to police, unless rules on traffic data retention was adopted. Since this is believed not only to be the actual situation in Denmark, the Ministry of Justice can support the solution of creating an instrument on traffic data retention for law enforcement purposes also at a European level.
Finland	Since the directive leaves the data retention question open, it is hard to judge how it should be handled on the European level. On the national level the problems can be solved by obliging the operators to store the information for 2 years (now information gets stored for 3 months). That would be sufficient time for investigation of most criminal cases including economical crimes, complicated homicide investigations as well as investigations on crimes related to terrorism.
France	
Germany	The Federal Government will only be able to answer the question of whether it is desirable to create EU-wide framework regulations covering these issues if it is proved that there is a need for regulation at EU level because of substantiated shortcomings in cross-border law enforcement caused by differences in national provisions. In addition, the Federal Government must first determine whether and to what extent it is actually necessary, and permissible pursuant to German constitutional law, to require teleservice providers and suppliers of

Questionnaire 7: How would you rate the solution of creating an instrument on traffic data retention for law enforcement purposes at a European level?	
	telecommunications services to retain traffic data (see question 1 above).
Greece	
Ireland	We would favour the amendment of the Data Protection Directive in the telecommunications sector to ensure that law enforcement access to call related data is in accordance with national legislation.
Italy	<p>High Tech Crimes are, most of the time, international crimes. Therefore, international cooperation in the matter is always welcome. An efficient response to the menace posed by HTC has to take in the right consideration the need to avoid creation of "safe heavens" in civilized countries. This can also be achieved through the harmonization of the various legislations. Hopefully the hypothetical instrument should also allow a faster way to exchange information among law enforcements of the various countries involved in the investigation as well as a new, dedicated and standardized procedure for the collection and transmission of evidence.</p> <p>Ministry of Justice: <i>Omitted.</i></p>
Luxembourg	
Netherlands	<p>We have already referred under question 5 above to the investigation currently under way into the categories of data retained by telecommunications providers and the obstruction experienced by the criminal investigation and intelligence and security services because of the absence of an obligation to retain historical traffic data. The results will determine whether there is a need to introduce additional obligations to retain data. Article 8 of the ECHR must be taken into account in this context. The Netherlands delegation calls for consideration to be given to a legal instrument taking its legal basis from Title VI of the EU Treaty. Finally, we must refer to the draft Council conclusions on information technology-related measures concerning the investigation and prosecution of organised crime (10358/02 CRIMORG 49 MI 19). In the draft conclusions the Council urges, inter alia, that within the very near future, binding rules should be established on the approximation of Member States' rules on the obligation of telecommunications services providers to keep information concerning telecommunications in order to ensure that such information is available when it is of significance for a criminal investigation (conclusion 9). In this context, too, the Netherlands has pointed out that there are no further steps under discussion apart from the rules which are currently valid in the Netherlands. The Netherlands delegation considers that good coordination between these two approaches is also of great importance.</p>
Portugal	
Spain	Very highly.
Sweden	<p>The ability of law enforcement authorities to cooperate within the EU is essential in the fight against cross-border crime. The Council of Europe Cybercrime Convention establishes mechanisms for cooperation in this specific field, and it is difficult to see how that cooperation could be successful if the rules on traffic data retention seriously diverge among its signatory states, including the Member States of the EU.</p> <p>Actors at the telecommunications market are international. In our view a uniform European solution might lead to lower costs for operators and thus be easier to implement.</p>

Questionnaire 7: How would you rate the solution of creating an instrument on traffic data retention for law enforcement purposes at a European level?	
United Kingdom	To resolve these issues on a European basis would be very useful