EUROPEAN COMMISSION
Directorate General for Home Affairs

Final Report – Task 2

Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries

November 2012

Centre for
Strategy & Evaluation
Services

P O Box 159
Sevenoaks
Kent TN14 5WT
United Kingdom
www.cses.co.uk

Contents

Introduction 1

This document contains the final report on Task 2 for the "Research study into evidence of potential impacts of options for revising the Data Retention Directive", commissioned by Directorate-General Home Affairs (DG HOME).

The assignment was carried out as part of a framework contract with DG HOME on the provision of evaluation and evaluation-related services (HOME/2011/EVAL/01 (HOME/2011/ISEC/FC/017/A3).

1.1 Study Aims

The study was launched to inform the Commission's impact assessment and potential proposal concerning revisions to the current EU legal framework for storage, access and use of telecommunications data for the purpose of combating crime, more specifically Directive 2006/24/EC on 'the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks' and amending Directive 2002/58/EC (the "Data Retention Directive", hereinafter referred to as the "DRD").

The Terms of Reference set out two main tasks around which work was structured, namely:

- **Task 1**: Impact of policy options for amending the data retention framework;
- **Task 2**: Current approaches to data preservation in EU Member States and third countries.

This document contains the report on Task 2. A separate document has been prepared containing the report on Task 1, which also includes an overview of the methodology for the study.

The aim of Task 2 was, according to the terms of reference: *to examine how data preservation is applied within the EU and elsewhere, and how effective it has proven in criminal investigations. It will compare the role of telecommunications data which are available as a result of data retention obligations and those available as a result of data preservation. It will look in particular at how Articles 16 and 20 of the Budapest Convention on Cybercrime[1] (hereafter referred to as 'the Cybercrime Convention') has been implemented.*

Specific sub-tasks were as follows.

2A) Existing legal framework for data preservation

1. *List and describe the main features of legislation which is in place for data preservation in EU Member States, in the United States and in other third countries.*

2. *Describe how countries in the EU and elsewhere have implemented the provisions on expedited preservation of stored computer data (Article 16) and on real-time collection of traffic data (Article 18) in the Council of Europe Convention on Cybercrime (see background below).*

[1] http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

Introduction 1

2B) Effectiveness of data preservation as a tool

1. *Describe how data preservation is applied operationally in EU Member States, in the United States and in other third countries.*
2. *Assess the effectiveness and importance of data preservation as an investigative tool in these EU Member States, in the United States and in other third countries for combating crime.*
3. *Assess the cost of implementing data preservation.*

2C) Comparison of data retention and data preservation

1. *Describe data retention and data preservation as investigation tools.*
2. *Explain their differences in terms of access to data for law enforcement authorities, requirements for business, data protection and privacy interests.*
3. *Assess the extent (a) to which data retention and data preservation could be complementary and (b) to which data preservation, without data retention, could help achieve the same results in criminal investigations.*

In line with the terms of reference, and with the agreement of the Commission, Task 2 covered EU Member States as well as a selection of three non-EU countries (Norway, Croatia and the US).

The research was carried out between December 2011 and July 2012. It consisted of:

- A survey of operators, competent authorities and NGOs;
- An analysis of responses to a survey that was undertaken by the Council of Europe and sent to members of the Cybercrime Convention Committee ('T-CY') in order to assess the implementation of the Budapest Convention regarding preservation measures (Articles 16, 17, 29, 30) by state parties[2];
- A workshop held on 23 May 2012 involving Commission officials from DG HOME and DG JUST, representatives from the European Data Protection Supervisor (EDPS), the secretariat of the Council of the European Union, the Council of Europe, national delegates from the Netherlands, Germany, Italy, the US and Japan, and members of the study team; and
- Interviews with individual experts.

We are most grateful to the Council of Europe and in particular to Alexander Seger, Head of the Economic Crime Division, for their expert input and for sharing the results of their survey.

A total of 14 responses were received to the CSES surveys with operators and NGOs, of which 10 were from NGOs and 4 from operators. In addition a total of 15 responses to the Council of Europe survey were examined, including answers from twelve EU

[2] This was in response to the decision taken by the Cyber Convention Committee at its 6th Plenary Session 23-24 November 2011.

Introduction 1

Member States and the three covered non-EU countries that were submitted by May 2012[3]. The CoE also kindly circulated a questionnaire with supplementary questions that was prepared by CSES for the national contact points. Overall, nine EU Member States and two non-EU countries responded to this survey.[4]

The contract was held by the Centre for Strategy and Evaluation Services (CSES) with contributions from Deloitte.

1.2 Structure of the Report

This report examines data preservation legislation and procedures in comparison with data retention approaches.

More specifically, in addition to an introduction to data preservation, it reports on responses from stakeholders and experts. The document is structured as follows:

- **Section 2:** Background to Task 2, data preservation and data retention;
- **Section 3:** The existing legal framework for data preservation according to responses to the CSES survey and Council of Europe questionnaire;
- **Section 4:** The relevance and effectiveness of data preservation as a tool according to respondents to the survey and questionnaire;
- **Section 5:** Conclusions.

[3] EU Member States: Bulgaria, Estonia, Finland, France, Germany, Latvia, Lithuania, the Netherlands, Portugal, Romania, Spain and Slovenia. Non-EU countries: Norway, Croatia and the US.

[4] EU Member States; Bulgaria, Finland, France, Hungary, Latvia, Lithuania, Portugal, Romania and Slovenia. Non-EU countries: Norway and US.

2 Existing Legal Framework for Data Preservation

2.1 Data Preservation and Data Retention

Data *preservation*, also known as expedited preservation of stored data or 'quick freeze', refers to situations where a person or organisation (which may be a communications service provider or any physical or legal person who has the possession or control of the specified computer data) is required by a state authority to preserve specified data from loss or modification for a specific period of time (a maximum of 90 days under the Cybercrime Convention).

That person or organisation may then be required, often by means of a court order, to disclose those data, usually on the ground that the data relate to specific individuals who are suspected to be connected to a particular criminal investigation or prosecution. The data may concern any type of stored information, including the content of communications (such as an email or voicemail message) as a well as non-content data such as 'traffic data' (that is, the route, time, destination and source of a communication).

Data preservation therefore requires that data, which already exist in a stored form, are protected from external factors that would cause them to be deleted or their quality or condition to change or deteriorate. Preserved data or copies of those data may be accessed and used for legitimate purposes by authorised persons.

Unlike data preservation, data *retention* measures generally aim at requiring (some or all) operators to retain non-content data generated or processed as a result of activities of all users of operators' communications or network services so that they can be accessed by state authorities and used for 'public order' purposes when necessary and lawful.

It can be noted that data preservation is a requirement according to the Cybercrime Convention. Therefore, the Member States that have ratified the Convention have the obligation to implement both measures.

In the following section we provide an overview of the legal framework for data preservation at the international level and in EU Member States.

2.2 International Legal Framework - The Budapest Convention

At the international level, preservation of stored computer data[5] is covered by the Cybercrime Convention of the Council of Europe[6] (the "Budapest Convention"). This Convention entered into force on 1 July 2004. As concerns the current situation with regard to the signature and ratification of the Budapest Convention by the EU Member States, all EU Member States have signed the Convention; the last ones in 2005. Seven Member States, however, still need to ratify the Convention (CZ, GR, IE, LU, PL and SE)[7].

[5] 'Computer data' is defined (Article 1b) as 'any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function'

[6] http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[7] Last checked on 29 November 2012.
http://www.conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=16/11/2012&CL=ENG

2 Existing Legal Framework for Data Preservation

More than 100 countries worldwide have used the Cybercrime Convention in drafting their legislation. There is a strong interest in implementing both Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data[8] and the Budapest Cybercrime Convention. The Council of Europe is promoting both.

The main objective of the Budapest Convention is to promote a common criminal policy aimed at the protection of society against cybercrime, in particular by adopting appropriate legislation and fostering international co-operation.

The Articles relating to data preservation in the Budapest Convention are as follows:

- **Article 16** – Expedited preservation of stored computer data (domestic level);
- **Article 17** – Expedited preservation and partial disclosure of traffic data (domestic level);
- **Article 29** – Expedited preservation of stored computer data (international level);
- **Article 30** – Expedited disclosure of preserved traffic data (international level).

While Article 16 covers expedited preservation at the domestic level, Article 17 is focused on partial disclosure. The latter Article was established as a reaction to the fact that preservation may cover multiple service providers. Article 17 therefore allows for the entire chain of service providers (i.e. communication path) to be covered. Articles 29 and 30 are mirroring these Articles, however, covering the international level**.** The full text of the Articles is provided in Appendix G.

The four Articles - 16, 17, 29 and 30 - constitute provisional measures. The provisional measures have been put in place in order to gain time in situations where it is too time-consuming to make a request in line with existing formal procedures. According to stakeholders, this is particularly important at the international level, where the formal procedures are often rather lengthy.

In view of this, the data preservation provisions constitute provisional measures, and need to be considered in conjunction with Articles 18, 19, 31 and 23 of the Budapest Convention, which set out formal measures to obtain data. The scope of these Articles is as follows[9]:

[8] The purpose of this Convention is to ensure the respect for fundamental rights, in particular the right to privacy with regard to automatic processing of personal data ("data protection"). The Convention is the first binding international instrument that protects the individual against abuses of personal data and to regulate cross-border flows of personal data**.**

http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

[9] The full text of the Articles is provided in the Appendix.

Existing Legal Framework for Data Preservation

2

- **Article 18: Production order** - giving competent authorities the right to order the submission of specified computer data from natural or legal persons, based on that such data is in his/her possession or control, or subscriber information held by service providers;
- **Article 19: Search and seizure** - empowering competent authorities to search or access computer systems (or part of such) and computer data storage media as well as computer data stored therein. Article 19 also gives them the right to seize and secure this data;
- **Article 31: Mutual assistance regarding accessing of stored computer data** - allowing Parties to the Convention to search, access, seize, secure and disclose data stored by means of a computer system on their relevant territory. Responses should be made by means of relevant international instruments, including those set out in Article 23; and
- **Article 23: International cooperation -** Cooperation shall be made in line with relevant international instruments and in accordance with the principles set out in the Convention. The cooperation shall be made to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences that are related to computer systems, computer data and electronic evidence[10].

In this way, the provisional measures constitute a first step, followed by the formal measures.

An overview of national legislative frameworks which have been introduced based on these Articles is provided below. In some of the countries that answered the CoE survey, data preservation is specifically foreseen in procedural law, including four EU Member States (Bulgaria, France, Latvia and the Netherlands), Norway and the USA.

2.3 Legal Framework in EU Member States and non-EU countries

Below we provide an overview of data preservation legislation and procedures that are in place in the twelve EU Member States and three non-EU countries (Croatia, Norway and the US) that contributed to our research.

To illustrate similarities and differences between data preservation and data retention as approaches, some of the key elements are compared. The information concerning the implementation of data retention in the Member States is based on the Evaluation Report of the Data Retention Directive[11] that was published by the Commission in April 2011[12]. Rather varying information concerning the legal provisions in place in relation to data preservation was provided by the countries that responded to the surveys. Therefore, the exhaustiveness of the analyses provided below cannot be guaranteed; the fact that certain measures have not been mentioned for particular countries does not

[10] It can be noted that not only Article 23 contains relevant provisions on MLA.
11 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
[12] http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

mean that they are not in place, but merely that they have not been commented on in the answers to the surveys.

In the next sub-sections, the following elements of the legal frameworks concerning data preservation and data retention are considered:

- Criminal offences for which data may be preserved or retained;
- Types of data to be preserved or retained;
- Orders for data to be preserved and access to data;
- Disclosure of data;
- Preservation and retention periods; and
- International cooperation in relation to data preservation.

2.3.1 Criminal offences for which data may be preserved or retained

Data preservation under the Cybercrime Convention is broader than the Data Retention Directive in terms of the purpose for which data may be required to be stored. The Data Retention Directive requires operators to retain data for the purposes of the investigation, detection and prosecution of serious crime as defined in national law (Article 1). According to Article 14 of the Cybercrime Convention, data may be preserved "for the purpose of specific criminal investigations or proceedings". This limits the application of the measures to an investigation in a specific case, but the types of crime for which data may be preserved are not specified.

With regard to the situation in the EU Member States and non-EU countries, according to the results of the CoE survey, the data preservation provisions apply to electronic evidence in relation to "any criminal offence" in nine countries (BG, ES, FI, FR, LV, PT, RO, NO, US), while six countries indicated the scope is more limited (DE, EE, LT, NL, SI, HR). Examples of limitations include that only serious crimes are covered, although certain pre-trial investigations concerning less serious and minor crimes may also be covered.

In this respect it can, however, be noted that according to the Commission's Evaluation Report on the DRD, data retention measures in eight countries (BE, DK, FR, IT, LV, PL, SK and SI) apply a purpose limitation which covers all criminal offences, prevention or general grounds of national or state and / or public security. This goes beyond the limitation of data retention under the DRD to 'serious crime'.

2.3.2 Types of data to be preserved or retained

The DRD applies to fixed network and mobile telephony, Internet access, Internet email and Internet telephony. The categories of data to be retained are as follows (Article 5):

- The source of a communication;
- The destination of a communication;

- The date, time and duration of a communication;
- The type of a communication;
- Users' communication equipment or what purports to be their equipment; and
- The location of the mobile communication equipment.

Unsuccessful call attempts are also covered to the extent that data on these attempts are generated or processed and stored or logged by operators. No data on the content of the communication may be retained. Search queries are also outside the scope of the Directive, because they are considered as consent rather than traffic data.

Data preservation, as established in the Cybercrime Convention, has a broader scope in terms of the types of data to be preserved. More specifically, Article 16 of the Convention refers to "[…] specified computer data, including traffic data that has been stored by means of a computer system […]". A definition of traffic data is provided in Article 1(d) of the Convention. The categories of data covered include: the origin of a communication, its destination, route, time (GMT), date, size, duration and type of underlying service.

It is noted that not all of these categories will always be technically available, capable of being produced by a service provider or necessary for a particular criminal investigation. It is further explained that "origin" refers to a telephone number, IP address or similar identification of a communications facility to which operator provides services and that "destination" refers to a comparable indication of a communications facility to which communications are transmitted. The term "type of underlying service" refers to the type of service that is being used, such as file transfer, e-mail or instant messaging.

Therefore, one key difference between data retention under the DRD and data preservation under the Cybercrime Convention is that the latter provides for the storing of communication *content*, while the former explicitly excludes it. According to the survey results, all fifteen countries (BG, EE, ES, FI, FR, DE, LT, LV, NL, PT, RO, SI, HR, NO and US) that answered the CoE survey state that they are covering all types of data referred to in Article 16 of the Budapest Convention in their national legislation. None of the countries indicated that not all types of data are covered.

2.3.3 Procedures for data preservation

Under the DRD, data should be retained for all subscribers by "the providers networks" for a period of six to 24 months. SMEs are excluded from this requirement in Finland and UK.

Under data preservation there is no such general requirement to store data that are generated. For data to be preserved, an order has to be issued. As indicated above, some basic conditions need to be met for the issuing of an order. As concerns the situations in which an order for data preservation may be issued, most countries that provided relevant information made reference to different prerequisites (in addition to the type of crime for which data can be preserved; this is considered above). Examples of prerequisites mentioned are as follows:

2 Existing Legal Framework for Data Preservation

Examples of situations in which an order for data preservation may be issued

- In **Finland**, an order for data preservation may be issued where there is reason to assume that data, which might be of relevance for investigating an offence, will be lost or altered.
- In **the Netherlands**, reference is made to data that are particularly *vulnerable* to loss or change. However, according to a representative of the Dutch Ministry of Justice, while this may seem like a restriction in theory, it is not much of a restriction in practice.
- In **Romania,** data preservation is possible in urgent and justified cases, if there are data or 'substantiated indications' regarding the preparation or committing of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the suspects.
- In **Slovenia**, data may be preserved in cases where there are reasonable grounds to believe that a criminal offence has been committed, is being committed or is being prepared or organised, and information on communications using electronic communications' networks is needed for the detection of this criminal offence or identification of the perpetrator.
- In **Norway,** the prosecuting authority may make an order as part of an investigation if there is reason to believe that a criminal act has been committed and if the securing of electronically stored data is deemed to be 'significant' as evidence.
- In **Croatia,** data preservation is only possible where an investigation cannot be carried out in any other way or would be accompanied by great difficulties.

Two countries (FI and US) emphasised that a preservation order does not give the authority any right to obtain information concerning the content of the data.

As concerns the time taken to issue an order, half of the countries surveyed indicated that on average order were issued in less than 24 hours. Slovenia and Hungary stated that issuing orders can take seven to ten days because a judicial decision or court order is needed. Four countries (FI, PT, ES, US) did not indicate how long it takes on average to issue an order.

Half of the surveyed countries (BG, FI, FR, HU, LV, SI) stated that preservation needed to be initiated 'fast', which could mean 'within working hours', 'the same day', '4 hours to 4 days' or '3 days'. Four countries (NO, LT, US, RO) reported that there were no specific timeframes for initiating the process.

Turning to the recipients of the preservation orders, half of responding countries indicated that preservation orders were issued to service providers only, while the other respondents in addition serve requests also to other physical or legal persons.

- Six countries including five EU Member States (BG, RO, NO, SI, FI, PT) serve preservation requests to physical or legal persons other than service providers. Finland and Portugal stated that a preservation order can be issued to any person who has the data relevant to the criminal investigation in his/her possession.

- Three EU Member States and two non-EU country (EE, NL, ES, HR, US) do not serve preservation requests to physical and legal persons other than service providers.

In some cases, more than one service provider is involved in the transmission of a communication. Two different procedures for ensuring that data preservation is effected among all the service providers have been adopted by the Member States:

- Preservation orders are sent to all service providers involved in a particular case (BG, FI, FR, SI, NO, US); or
- A preservation order is sent to the main service provider who is then asked to forward the order (LV, HU).

In two EU Member States (LT, ES) there are no practices or rules for such cases.

2.3.4 Authorities responsible for data preservation orders and requesting disclosure of data

The Cybercrime Convention (Article 35) requires a 24/7 contact point to be designated to provide assistance in investigations and in the collection of evidence. These contact points may issue or facilitate issuing and execution of orders. All Parties to the Convention have designated 24/7 contact points. These are as follows:

EU Member States

- Bulgaria: Cybercrime Section, Chief Directorate for Combating Organised Crime, Ministry of the Interior;
- Finland: National Bureau of Investigation Alternative CP: Ministry of Justice
- France: Office Central de Lutte contre la Criminalité liée aux Technologies de L'Information et de la Communication (OCLCTIC) Judicial Police, Ministry of Interior;
- Germany: National High Tech Crime Unit, Federal Criminal Police Office (BKA);
- Latvia: Operational Coordination and Information Provision Unit, State Police of Latvia;
- Lithuania: Cybercrime Unit, Lithuanian Criminal Police Bureau;
- The Netherlands: National High Tech Crime Unit (NHTCU), National Police, National Prosecutor Office;
- Portugal: Coordinator of Criminal Investigation in Portugal, Judicial Police;
- Romania: Service for Cybercrime, Directorate for the Investigation of Organised Crime and Terrorism Offences, Prosecutor's Office attached to the High Court of Cassation and Justice, Alternative CP: Cybercrime Unit, General Directorate for Countering Organized Crime and Anti-drugs Bucharest, Romania (National Romanian Police);
- Spain: Brigada de Investigación Tecnológica, Comisaria General de Policia Judicial, UDEF Central, And: Guardia Civil (GC), Grupo de Delitos Telematicos (GDT) (Computer Crime Unit);

Existing Legal Framework for Data Preservation

- Slovenia: Sector for international police cooperation, Criminal Police Directorate, Alternative CP: Cyber Investigation Unit, Criminal Police Directorate.

Non-EU countries

- Croatia: Department for Economic Crime and Corruption, General Police Directorate;
- Norway: High-Tech Crime Division, KRIPOS National Criminal Investigation Service (NCIS Norway); and
- USA: Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice.

Examples of the role and tasks of various authorities are provided below.

In **Latvia**, a decision is prepared and communicated to service providers by investigators. The investigators are also responsible for controlling the preservation procedures.

In **Slovenia**, different approaches are used depending on whether the suspect is known to the police or not. If the suspect is known, the police may make a written request to the investigating judge, who may then issue an order to the operator. If the suspect is unknown, the police must make a written request to the public prosecutor, who will send the written request to the investigating judge. In emergency cases operators are usually asked to preserve data before the judge order has been issued.

In **Croatia**, the State Attorney is responsible for making requests "in an integral, original, legible and understandable format". The State Attorney stipulates the terms for handing over the data requested. Based on a motion of the State Attorney, the investigating judge may, by means of a ruling, decide on the protection and safekeeping of all electronic data covered, as long as necessary but for a maximum of six months. After this term data shall be returned, unless certain conditions are met (e.g. the data relate to other criminal offences).

In **Bulgaria** and **Estonia** a police order is used and in **Spain** the judicial authorities involved may make the request.

In **Germany** an emergency order is executed through an announcement to the data subject (if present) and by subsequent seizure. In non-urgent cases, the public prosecution office - where requested by the investigating police unit - examines the necessity, proportionality and other legal conditions. If all prerequisites are met an appropriate motion is lodged to the relevant court. The court then itself reviews the facts of the case and if satisfied, may then order seizure of the data by the investigating police unit.

For preservation requests judicial warrants should not be necessary – that is the purpose of the provisional measure to preserve under the Cybercrime Convention – to give LEAs time to seek a judicial warrant for actual disclosure or production of preserved data. Judicial warrants for accessing data are necessary in all responding countries. In the **Netherlands**, request may initially be in writing or be verbal, but where it is verbal, it must be followed by a written request within three days. Only five countries (BG, FI,

FR, HR and US) stated that a standard template or form is used for making the requests. In **France**, two different forms are used depending on whether the case is urgent or "normal" (*requisition judiciare*). In **Bulgaria** a standard police order is used. In **Spain**, "judicial models" are used. Seven countries (DE, EE, LV, PT, RO, SI, NO) stated that no such templates or forms exist. However, **Romania** and **Portugal** listed a number of details that normally are required when making a request[13].

Finally, it can be noted that seven countries (DE, LT, NL, PT, RO, NO and US) made explicit reference to the role of the prosecutor[14].

2.3.5 Access to preserved and retained data

As concerns the **access to preserved data**, in some countries prosecution authorities may gain direct access to data, while in others disclosure of content data and content related data is possible only with court order or judicial decision.

In **Germany** the prosecution authorities may gain *direct access* to computer data and data media to ensure their availability for use in criminal proceedings; these authorities may either take the data into official custody or take copies of the data from the storage media. The public prosecution office and the police are entitled to order seizure in urgent cases.

In **Lithuania** the police may also gain direct access; agreements are in place between the police and the largest national providers allowing police direct access to databases where necessary to identify the source of communication (i.e. name, surname and address of a subscriber or registered user of electronic communications services to which an Internet Protocol (IP) address was given during a process of communication).

In Bulgaria, Finland, Latvia and Norway data security requirements are not specified. However, in Bulgaria the data may be copied or preserved once the order has been approved but before it is received by the service provide. In Latvia the data is also copied but stored in a separate location from the original data.

Disclosure of content data and content related data is possible only with court order or judicial decision (HU, LV, SI).

Certain countries (BG, FI, FR, HU, LV, PT, RO, NO) indicated that some types of data including traffic data, content data and customer identification data are particularly vulnerable to loss or modification.

In relation to internal access to preserved data, in Lithuania only authorised personnel may access preserved data[15] and in Latvia there is a requirement to ensure the *inaccessibility* of data to other users of the system.

[13] Romania: The name of the issuing body, case file, date, facts, order to preserve, the data to be preserved, the period (starting day- ending day), the provider/person's, obligation to keep confidentiality, obligation to keep and preserve integrity, other information (contact person/address/phone etc). Portugal: The nature of the data that should be preserved, the origin and destination of those data, if known (in case of traffic data), and the period of time covered by the preservation order.

[14] Further details on the role of the prosecutor in these countries are provided in Annex B.

Existing Legal Framework for Data Preservation

2

As concerns the **access to retained data**, the DRD does not set out specific requirements concerning access to data; this is left to the Member States. More specifically, the Member States are, according to Article 4, required "to [ensure] that retained data are provided only to the competent national authorities in specific cases and in accordance with national law". The Member States should define the procedures and conditions that are to be fulfilled to access data in accordance with necessity and proportionality requirements. The Evaluation Report on the DRD observed the following variations:

- **Judicial authorisation** is required for all requests in eleven Member States and in most cases in a further three countries.
- **Authorisation by a senior authority** but not a judge is required in another four Member States.
- **Requests must be in writing** in two Member States.

The following stakeholders are authorised to access data:

- Police in all Member States which have transposed the DRD.
- **Prosecutors** in all Member States except for the common law countries UK and Ireland.
- **Intelligence services or the military** in fourteen Member States.
- **Tax and / or customs authorities** in six Member States.
- **Border authorities in** three Member States.
- **Other public authorities designated in secondary legislation** in one country.

2.3.6 Disclosure of preservation of data to the data subject

There is at present no obligation to inform subscribers about data retention or about individual requests to access retained data relating to a particular subscriber.

In relation to data preservation, in most Member States that answered the survey, it is possible to prevent disclosure of the preservation request to suspects. In four countries, (FI, LV[16], PT, SI), the natural or legal person receiving the data preservation order is obliged to keep it confidential. In **Finland** and **Latvia** it is punishable to

[15] This data must be of the same quality and subject to the same security and protection as the network data and be subject to "appropriate technical and organisational measures" to protect the data against accidental or unlawful destruction or accidental loss or alteration, unauthorised or unlawful storage, processing, use or disclosure.

[16] However, in Latvia the situation in relation to disclosure of data is different in relation to pre-trial criminal proceedings, where the person directing the proceedings may request in writing, based on a decision of an investigating judge or with the consent of a data subject, that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in the relevant law.

disclose such information. Other countries, however, indicated that it is not necessary 'in principle' to inform suspect(s) of preservation orders in advance (DE, FR) or that there is 'no obligation' to inform suspects (RO).

As concerns the non-EU countries covered, in **Croatia** evidence is not visible when applying 'special evidence collecting measures' and in the US most major providers generally do not disclose preservation to the account holder upon requests from the government. In **Norway** there is, however, an information obligation; the suspect shall be informed as soon as the data has been secured and s/he has been given the status of a suspect. If necessary for the purpose of the investigation, the courts may, however, give the police the right to defer providing information to the suspect and/or to the account holder.

In nine responding countries (BG, FI, FR, HU, LT, NO, PT, RO, ES), under national laws companies or persons subject to data preservation orders are either obliged or may maintain confidentiality of preservation orders. In two EU Member States (LV, SI), there is no law in place for ensuring confidentiality of data preservation orders but the person subject to the preservation order is requested to maintain the confidentiality of the order. In the US there is no confidentiality requirement but in practice subscribers are not informed where data relating to them is preserved.

2.3.7 Preservation and retention periods

The DRD requires Member States to ensure that certain data are retained for a period of between six and 24 months. Under the Cybercrime Convention, the person subject to a production order is obliged "to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure." A maximum preservation period should be established in national legislation. Furthermore, the order should specify the exact period of time that the specified data is to be preserved. This time period should be as long as necessary up to maximum 90 days, in order to allow the competent authorities to undertake other legal measures, such as search and seizure, similar access or securing or the issuance of a production order.

According to the responses to the survey:

- **Two EU Member States (LV, PT) provide for a maximum of 30 days preservation** with a possibility to extend the preservation for up to an additional maximum 30 days (LV) or a maximum one year (PT).
- **In the Netherlands, data may be preserved for 45 days**, renewable once[17].
- **In Bulgaria, Finland, Romania, Norway and US data may be preserved for maximum of 90 days or three months which may be extended for an additional** maximum period of 30 days in Romania (RO) or three months (Finland). In the US this period may be extended for additional 90 days periods.

[17] This information was given in the workshop on data preservation on 23 May 2012.

- In **Lithuania**, the data should be preserved for six months. The response from Croatia indicated a maximum time period of six months.

BG, NO, HU, FR, ES, LT indicated that there is no limit or set number of renewals of orders established in law.

2.3.8 International cooperation in relation to data preservation

While the DRD does not include any provisions for cross-border data exchange, Article 29 of the Cybercrime Convention stipulates that Parties may request data from each other and establishes the type of information to be given in such a request[18]. The country receiving the request must take all appropriate measures to preserve data expeditiously in accordance with its national law. The minimum length of preservation is 60 days.

Generally, international preservation requests are received by the 24/7 contact points who orders a service provider or other legal or physical person to preserve data. When a formal request for MLA has been received and a court order has been issued, the service provider discloses the data to the domestic authorities who then transmit them to the requesting Party.

The role of the 24/7 contact points is to receive requests from other contact points (FR, DE, LT, NL, US) and act as an interface between service providers and local / foreign competent executing authorities (FR, DE, NL), normally the police. In one country (SI) the role of the contact point has been stated to be to provide technical and practical advice. In this regard, it can, however, be noted that all contact points have this obligation according to Article 35 of the Cybercrime Convention.

Below an example of how a request is handled in Romania is provided. This procedure (with adjustments to specific domestic conditions) is followed by a number of Parties, in particular where preservation powers are specifically defined by law.[19]

International Expedited Preservation Requests: Example of Romania

- An international expedited preservation request sent to the Romanian 24/7 Contact point (via email) is describing a case of intrusion followed by alteration of data. The case is investigated by a local police office in country X. The Romanian authorities are asked to preserve subscriber information and traffic data related to several IP addresses (time and date indicated). According to the letter IP address belong to a provider located in Bucharest.

[18] This includes: the authority seeking the preservation; the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; the stored computer data to be preserved and its relationship to the offence; any available information identifying the custodian of the stored computer data or the location of the computer system; The necessity of the preservation; and that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data

[19] Cybercrime Convention Committee (T-CY): *Assessment Report - Implementation of the preservation provisions of the Budapest Convention on Cybercrime* (Draft).

- After registration in the unit's register, the prosecutor will verify the IP addresses and the provider and then will issue the ordinance for preservation.
- If the information provided by the requesting country is not accurate or the provider no longer exists (even if the company is still mentioned on RIPE etc.), the prosecutor will inform the other party to rectify the request.
- The requesting country is also informed that for getting the information that was preserved a letter rogatory is needed.
- A territorial office in Romania is asking the 24/7 Contact point to forward its expedited preservation request to country X. The local request is describing the facts, specific crime, and is asking for preservation of subscriber information related to an email address (service based in country X) and the login information for a specified period of time. It is also requested the preservation of the email box content.
- The request will be registered in the unit's register and with a cover letter will be sent via email by the Romanian 24/7 Contact Point to the foreign 24/7 Contact Point.

It can be noted that of the countries examined, only France indicated that two standard forms are used during this process.

As concerns the timeframe for receiving a notification that a request has been issued in the foreign country, most (BG, FI, FR, LV, RO, ES, NO, US) **of the responding countries stated that they are notified within one day.** Bulgaria stated that notification could take up to three days.

With regard to the use of MLA, the Netherlands, Romania and Norway reported that most international data preservation requests were followed by mutual legal assistance requests, while Bulgaria, Croatia and US stated that this was not the case in their experience.

Ten countries (FI, FR, DE, EE, LV, NL, RO, SI, HR and US) reported that mutual legal assistance rules applied to requests for transfer of preserved data. France and Germany indicated that foreign authorities were required to submit an official request for judicial cooperation in order for data to be transferred.

2.3.9 Data preservation: penalties in case of non-compliance

Hungary and United States reported that there are no specific penalties for non-compliance.

In other countries, penalties can be applied for failure to ensure security or confidentiality of data (Slovenia, Finland, Latvia, Romania), delays in disclosing the data requested or failure to disclose the data (Croatia).

The types of penalties reported included community service, fines or restriction of liberty (Lithuania), fines of between 50,000 and 400,000 EUR (SI), fines and/or up to three months imprisonment (NO) and two years of imprisonment or a fine of maximum 240 days (PT).

Effectiveness & Relevance of Data Preservation 3

The previous section set out the legislative and procedural frameworks in the Member States and selected non-EU countries. This section concerns the effectiveness of data preservation by examining its implementation in practice.

3.1 Frequency of use

The national surveys included questions on the frequency of use, relevance, and the strengths and weaknesses of data preservation. The results are presented below.

Turning to the first of these issues, whilst the responding countries generally saw a need for and relevance of data preservation, the instrument seems to have only been used to a rather limited extent. When used, data preservation is currently more used in cross-border cases than in national cases. To illustrate the use of data retention and data preservation, the example of the Netherlands can be taken:

> In the Netherlands it was estimated that 100-150 cases were handled in 2011. The number has increased over the last two years. All of these cases were cross-border. No official statistics are, however, available. This can be compared with the number of requests for retained data, which amounted to approximately 85,000 in 2008. Almost all of these were stated to be needed for national purposes. As concerns the reasons for these differences, reference was made to the different types of data needed as well as a possible lack of awareness of data preservation in the police. In other words, one request for preservation corresponds to approximately 1,000 requests for retained data.

3.1.1 Frequency of use in investigations at domestic level and in relation to partial disclosure (Articles 16 and 17)

With regard to the frequency of use of data preservation under Article 16 only four countries (two non-EU countries and two EU Member States) were able to provide estimates. The figures given differ significantly; three requests per year were indicated by one non-EU country, an estimated 100 requests in two EU Member States and "thousands" of requests in one non-EU country. Three EU Member States stated that data preservation is never or only rarely used. Eight countries including seven EU Member States reported that no statistics were available.

Only very limited information is available on the frequency of use of Article 17. One non-EU country and one EU Member State pointed out that the provisions of partial disclosure are often used. The non-EU country further indicated that subpoenas for partial disclosure of traffic data and subscriber information can be estimated to be in the thousands each year. One EU Member State and one non-EU country indicated that the provisions are rarely used, and another Member State stated that the provisions have so far never been used. Three EU Member States indicated that no information is available and one EU Member State pointed out that there are no statistics available because partial disclosure is not used.

3.1.2 Frequency of use in investigations at international level (Articles 29 and 30)

Although it can be concluded that more use is made of data preservation in international cases than national ones, five Member States indicated that international preservation orders are only sent and received very rarely.

- Of these, four countries send and receive one to five requests per month. The fourth country indicated that they had only sent two to three cases up until now.
- One Member State reported that international preservation orders are sent and received through official channels (i.e. from a police authority in one country to a police authority in another country) very rarely. Instead, most requests are sent directly to large international private companies who in follow their own internal policies in determining whether to provide the data requested directly to the requesting authority.
- The two non-EU countries that have responded to this question of the survey stated that they see an increase in the number of requests, although only one of these countries was able to provide any estimates of the number of requests. In one of these countries, the competent authority processes "hundreds of international preservation requests each year".

Five Member States and one other country stated that no national statistics were available.

Explicit information concerning the frequency of use of Article 30 is only available for one Member State, which sent such a request more than ten times, but the requested Party did not disclose the data. Two other EU Member States indicated that they use the provisions "often". In three EU Member States and one non-EU country Article 30 was stated to be "rarely used" and in one non-EU country it has never been used in practice. One non-EU country pointed out that one specific service provider receives a high number of requests from other countries. Four EU Member States indicated that no information is available.

With regard to the reasons behind the current limited use various possible reasons were put forward by experts: a lack of specific regulations; a lack of efficient procedures; a lack of experience/know how; direct search, seizure, production orders being more efficient; historical data are missing; a reliance on data retention; and complicated follow up through MLA at the international level.

Capacity building and awareness-raising were considered to be key for the future, as well as electronic training. One of the workshop participants pointed out that the situation in LEAs is better with regard to telecommunications than the Internet, which is still very much a niche. In general, statistics on cybercrime show that it is rising at a fast pace, so that it is very difficult for LEAs to keep up with it. In addition, the scope of investigations using telecommunication data is broadening, and so does the request for training on these forensic tools.

3.2 Relevance of data preservation

Feedback from the research, in particular the individual experts who were interviewed, suggested that data preservation is an important tool for ensuring access to data as part of investigations in terms of preventing that the relevant data is deleted. These data can then be used as evidence. The same experts confirmed the conclusions of the workshop in terms of that data preservation has become increasingly more relevant in recent years in view of technological developments and the increasing use by criminals of telecommunications, including e.g. mobile telephones, and is likely to become even more relevant in the future.

As concerns the relevance of data preservation in relation to investigations, certain experts argued that data preservation was mainly relevant in international cases and hardly used in domestic cases. Search and seizure is instead made use of in domestic cases:

- Five EU Member States and two non-EU countries stated that data preservation is a key action for successful investigations.
- According to four EU Member States, due to the volatile nature of computer content data, data preservation may ensure its availability for investigation purposes.
- One EU Member State said that data preservation was not relevant for domestic investigations.

Responses generally indicated that preserved data where accessed often gave investigators sufficient additional facts to obtain a court order or search and seizure warrant compelling service providers to disclose all traffic data or traffic data plus content data, and enabled identification or location of a suspect or witness. Experts stated that traffic data was necessary for a large number of investigations.

3.3 Effectiveness of service provider cooperation

The survey included a question on how the cooperation with service providers in the execution of preservation requests is rated in relation to the implementation of Article 16. In eight countries, of which one non-EU country, the cooperation was rated as good/efficient or even very good. One non-EU country stated that in most cases the cooperation runs smoothly, but some service providers have raised issues regarding the wording in the preservation order. Three countries including two EU Member States reported cooperation to be rare or non-existent.

The general response time by service providers were indicated to vary from a day to a week in three EU Member States, while in two other Member States it takes a day to a couple of weeks. According to the three non-EU countries that answered this question the response times were very prompt (less than a day to a few days). Six EU Member States were unable to answer the question.

Ten of the 14 countries surveyed (BG, LV, PT, NO, SI, ES, PT, RO, HR, US) reported that there were no agreements or voluntary arrangements in place

between law enforcement authorities and service providers or private sector holders of data. Such an agreement was only in place in EE and LT, and was under discussion in Portugal.

3.4 Key strengths and weaknesses

Based on the above, data preservation is appropriate in situations when a suspect has been identified. However, when there are no suspects, this approach is, at least by some, considered to be inappropriate. Indeed, preservation has been criticised for not allowing investigators to examine historical trends and patterns which can lead to the identification of actors involved in a crime. Some stakeholders are of the view that it could even be seen as more intrusive than data retention, since it allows the examination of the content of communications, which is not covered under data retention schemes. At the same time, data preservation is often considered to be less intrusive than data retention, since it is used in relation to specific suspects and provides a snapshot of the situation, rather than obliging operators to retain data for all users.

Table 3.1: Summary – Strengths and Weaknesses of Data Preservation

Strengths	Weaknesses
• The preservation order is simple and quick to issue and enforce. • Data preservation is the only way to prevent the deletion or modification of computer data needed for cybercrime investigations and that is not subject to data retention requirements • Data preservation ensures that data is kept during lengthy mutual legal assistance procedures	• Lack of knowledge of data preservation among judiciary, including conflation of data preservation with lawful interception • Cooperation between law enforcement agencies and operators/service providers is not always satisfactory and reaction times can be slow and thereby jeopardise the success of the investigation. • Usually there is no standard format for requests and protocols • The procedure for international preservation orders is often too long and complicated. The requested data may not be received.

The respondents were also asked if problems for international cooperation would result if there were no provisions on preservation. Eleven countries, of which eight EU Member States and three non-EU states, agreed that the provisions were adequate and that without the Convention international cooperation would be hampered.

Costs for operators

Generally, the same factors that affect the costs associated with data retention lead to costs for operators in relation to data preservation, including the types of data to be kept and data protection and data security requirements.

4 Findings - Data Preservation & Data Retention as Alternative or Complementary Instruments

In this section we compare data preservation and data retention as methods and present overall conclusions.

4.1 Data Preservation and Data Retention Compared

To clarify the differences between data preservation and data retention, the key elements of the two instruments were compared in the following way in the expert workshop that took place as part of Task 2 of the assignment:

Table 4.1: Differences between data preservation and data retention under the DRD

Element	Preservation	Data retention
Aim	Expedited preservation of volatile evidence to allow for time for formal measures to obtain evidence	Ensure that data is available for investigation, detection and prosecution of serious crime
Mechanism for maintaining data	Order preservation of specified data	Automatic retention of data
Type of data covered	Stored computer data	Traffic data, location data and subscriber information
Coverage of crime	Any crime	Serious crime as defined under national law
Actor required to store data	Any physical or legal person	Publicly available communications service and network providers

Source: Based on the Council of Europe presentation at the 23 May 2012 workshop

Experts considered that there was **confusion among stakeholders about the distinction between data preservation and data retention, for example, in terms of that the two approaches are considered to be alternatives**, and that one can be used instead of the other. **More awareness raising was needed to bring clarity to the aims and intended use of the two instruments.**

Findings - Data Preservation & Data Retention as Alternative or Complementary Instruments

4

4.2 Summary of Findings

The research suggests that data retention and data preservation are complementary rather than alternative instruments. More specifically, in the workshop the participants pointed out that notwithstanding the above differences, data retention plays a role in ensuring that data is kept and that this is sometimes a prerequisite for data preservation, as data may have already been deleted before a data preservation order is issued.

Two Member States stated that identifying suspects and their locations and suspects' activities would be more difficult in the absence of data retention. It was also pointed out that the two instruments concern different types of data. The reason behind data preservation is the need for information about the content of the communication, which cannot be provided under data retention.

According to one Member State, data retention data is more suitable for older data, but lacks content information and traffic data is still only the basic set of traffic data. In contrast, data preservation is a more extensive measure which allows the preservation of content and other traffic data which is not preserved with data retention.

Furthermore, the two instruments ensure that data are available during different time periods. In case the retention period is about to end, data preservation can further ensure that the data is maintained also after the retention period has come to an end, which leads to increased certainty that the data needed are available to LEAs. In the national survey, one of the countries pointed out that the more time that has elapsed from the committed crime, the fewer results one can expect from data preservation because the data are likely to have been deleted.

Respondents were unable to address the question of whether data preservation and data retention would yield equivalent results for a given investigation. It appears that where data retention measures are in place, there is less need for data preservation, unless data is required which are approaching the end of the statutory data retention period.

Only a few relevant examples were highlighted in the workshop and the surveys of where both instruments led to comparable results (sufficient evidence).

With regard to the point concerning the seemingly limited use of data preservation to date (see the previous section on effectiveness), based on the national survey, there seems to be a greater need for data preservation in cross-border cases compared to national cases, because it ensures that data are available at the end of often **lengthy mutual legal assistance procedures.**

While agreeing on the fact that more practical experience may be needed in relation to data preservation, the workshop participants concluded that **the two instruments data retention and data preservation are becoming increasingly important in view of the increasing trends of cybercrime and the necessity of electronic evidence also in relation to other crimes**. The development of transnational crime

Findings - Data Preservation & Data Retention as Alternative or Complementary Instruments

4

also needs to be taken into account, as well as the positive obligation of States to protect the society and ensure security when considering the two instruments. This is also important to take into account when discussing the issue of proportionality; data protection and privacy are not the only rights that need to be ensured. The availability of data may also be helpful for identifying and preventing attacks; some examples were given, including of botnets which are followed by some major providers.

In the workshop the issue concerning whether the EU should have a common approach on data preservation was also raised. According to the participants, the Cybercrime Convention was sufficient, but it needed to be promoted and ratified, and more efforts should be dedicated to raising awareness about how it should be implemented.

Finally, with regard to impacts on data protection and privacy, respondents from three countries (two Member States and one non-EU country) noted that both instruments had an impact on the fundamental rights to data protection and privacy, but that their field of applicability differed.

Some experts and NGOs stated that while a system of data preservation and targeted data collection had a lesser impact on fundamental rights, a risk remained in particular in view of that content data may be preserved as well as sensitive information about social contacts (including business contacts), movements and private, sometimes health-related contacts (e.g. with physicians, lawyers, workers councils, psychologists, helplines, etc.).