ROOM DOCUMENT

EVALUATION OF DIRECTIVE 2006/24/EC AND OF NATIONAL MEASURES TO COMBAT CRIMINAL MISUSE AND ANONYMOUS USE OF ELECTRONIC COMMUNICATIONS

TABLE OF CONTENTS

1. Introduction

Article 14 of the Data Retention Directive (DRD) states that the Commission shall submit to the European Parliament and the Council an evaluation "*of the application of the Directive and its impact on economic operators and consumers, taking into account further developments in electronic, communications technology and the statistics provided pursuant to Article 10 DRD, with a view to determining if provisions, in particular Article 5 or 6, should be amended*".

Moreover, the JHA Council of 27 and 28 November 2008 requested the Commission to evaluate the effectiveness of (non-)legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phones with prepaid SIM cards (cf annex 8).

The Commission carried out this mandate as reported below. The conclusions and main recommendations are contained in chapter 3; a full list of recommendations is included in the annex.

a. Procedure

The evaluation started on 14 May 2009 with the conference "Towards the Evaluation of the Data Retention Directive" that was attended by 140 representatives from relevant stakeholder groups: law enforcement, and data protection authorities, the private sector, academia and civil society who took stock of fundamental rights', law enforcement and technology issues to be addressed (see annex 3).

On 10 September 2009 representatives of MS and of EEA countries met in the Secure Zone of the Directorate General JLS to discuss the modalities of the evaluation, and were asked to comment the draft questionnaire.

On 30 September 2009, the Commission sent out the questionnaire contained in Annex 4 to all stakeholder groups, the European Parliament and industry associations taking. Until January 2010 it received [70] replies that are contained in annex 5 to the extent they were not classified.

During the same period, the Commission met with each MS and EEA country except for IT[1] to discuss the legal, practical and technical implementation of the DRD along the lines of the questionnaire (see Annex 7). The Commission debriefed MS and EEA countries on 23 November 2009 about the ongoing evaluation. On 12 March it asked them for comments on the present report, and representatives of stakeholder and with the Expert Group were organised on 12 March and 17 March 2010 respectively to assess the factual foundation and correctness of the information contained in this report.

b. The Expert Group "Platform on Electronic Data Retention"

By Decision of 25 March 2008, the Commission set up the Expert Group "Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime"[2] ("Expert Group") that advises on issues relating to data retention, and assists the Commission in identifying difficulties concerning the technical and practical implementation of the Directive, its evaluation as well as its impact on economic operators and consumers.

The Expert Group consists of representatives of MS law enforcement authorities, associations of the electronic communications industry, Data Protection Authorities and the European Data Protection Supervisor, and Members of the European Parliament.
In 2009, the Expert Group adopted five 'Position Papers' that provide a non-binding, authoritative interpretation of issues relating to the implementation of the DRD such as, f.i. whether or not log files regarding SPAM email should be retained, the application of the Directive to Web Mail and web-based

---

1 See Annex 1 for the abbreviations

2 Commission Decision of 25 March 2008 setting up the 'Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime' group of experts (2008/324/EC) OJ L 111/11 of 23 4 2008

messaging, and the role of third party networks and service providers (see the website of DG JLS http://ec.europa.eu/jls .....)
The Expert Group, met for the first time on 28 November 2008, three times in 2009 (16/3, 10/7 and 3/12), on 12 March 2010 and will have further meetings in 2010.

c. Statistics

According to Article 10 DRD, MS shall ensure that the Commission is provided on a yearly basis with on the retention of data generated or processed in connection with the provision of publicly available communication services or a public communications network.

The template for the communication of statistics was designed by the Expert Group and submitted for comments to Member States on 22 January 2009. It allows for a standardised collection of comparable information about the application of the Directive in the MS. The questionnaire contained quantitative questions that complemented the statistics of Article 10. Annex 6 contains the statistical overview based on data that only 12 MS provided.

Article 14 DRD stipulates that the Commission shall take the MS' statistics into account in the context of the evaluation, in particular to assess whether it is necessary to amend the list of data in Article 5 and the periods of retention provided for in Article 6.
The incomplete statistical data affects assertions as well as the conclusions. A number of MS reported that the decentralised access to retained data renders compilation of national statistics difficult. Others highlighted that the template deviates from the data categories requires a different collection. In many cases, the delayed transposition of the Directive signifies that data over 2008 or 2009 were not yet available.

The interpretation of statistics to assess the application of the Directive is furthermore hampered by the fact that national statistics mostly relate to requests for traffic and location data with the exclusion of subscriber and user data. However, the evaluation showed that latter data seem to be accessed (much) more frequently and under less demanding conditions than traffic or location data.
The major change that the DRD brought about was that providers of publicly available electronic communications services or providers of public communications networks (hereafter referred to as operators) had to retain traffic and location data; subscriber and user data (name, and address of a subscription-based fixed of mobile phone number or internet access, see Article 2(a) and (b) DRD – hereafter referred to as subscriber data), were already retained - and accessed by law enforcement authorities - because these data are the cornerstone of their business administration.
Moreover, some statistics refer to the number of criminal cases/proceedings in which data were requested, other to the number of requests, and other to the number of data that were obtained.

d. The structure of this report

This presentation of the results of the evaluation in chapter 2 of this report follows the structure of the questionnaire and maintains the division in four stakeholder groups. The purpose is to assess whether the **security** that the DRD aims to contributes to is **sustainable** and provides added value for all stakeholders groups. The obligation to retain data and keep them available must noticeably facilitate law enforcement action and apply even-handedly across the EU so as to create a level playing field for the private sector, whilst the data security must be such as to protect data from loss, unauthorised disclosure, misuse, alteration, or destruction. Essential are: making technology available to consumers at competitive prices, offering law enforcement authorities the tools to efficiently and effectively offset security risks whilst respecting the privacy of end-users. Security and privacy should converge to the protection of the same values. The Commission is committed to dialogue between the public and private sector, between end-users and suppliers, to ensure that technology tackles crime and ensures legitimacy[3].

---

3 http://ec.europa.eu/justice_home/news/events/conference_public_security_privacy_technology/docs/speech_tlm_jls.pdf

2. Evaluation

This chapter is subdivided in two parts: Part A that covers the evaluation of the DRD and Part B the evaluation of national measures to combat the criminal misuse and anonymous use of electronic communications (see annex 8).

PART A: Evaluation of the DRD

I. Law enforcement issues

1. national requests: number – authorities involved – age of data - procedures

The statistics in Annex 6 show that the amount of requests for retained data varies significantly between MS: from less than one hundred to half a million requests for traffic and location data on an annual basis. The differences have multiple, yet not precisely correlated causes such as the size of the population, types of crime for which data can be requested, modalities and conditions for access, and the costs for the acquisition of data. Some MS report not to avail of data (e.g. BG).

The numbers have a tendency to increase on a year-to-year basis. Operators are prohibited in certain MS to provide data that are older than the legal retention period, even if these data are retained for longer periods for commercial reasons (e.g. DE, FR). In other MS these older data, if available, must be provided (e.g UK).

In about 75% of the cases police authorities are competent to request data, followed by customs, financial crime investigating (banking) authorities, and judicial authorities (a prosecutor or an investigating judge). Officials other than judicial authorities must obtain authorisation from the latter. Many MS accommodate however for urgencies by allowing law enforcement to request data directly from operators and obtaining the authorisation soon thereafter. If authorisation is not given, the data that was obtained must be deleted. In the course of the bilateral meetings the Commission found that in many MS, access to subscriber data and the most recent in particular, underlies less strict conditions than traffic and location data and can be obtained by foreign colleagues without rogatory commission.

Although outside of the scope of the DRD[4] state security services of the majority of MS can gain access to retained data, mostly under similar conditions as law enforcement authorities. Few MS included this access in the statistics. One Member State reported it makes up 7% of its total requests.

The average age of the traffic and location data at the moment they are requested is between 3-7 months (mobile phone data tend to be the younger), peaking in the first three months. Some detailed statistics show a peak just before the end of a six month retention period (e.g. DE). This may be different for subscriber data because they are generally available for longer periods, in principle for the duration of the subscription with the operator. The detailed overview that LT provided seems to correlate the investigation of certain crimes with the age of data that are used; the investigation of counterfeiting, cyber crime, or trafficking of human beings relies on data that are up to three times as old those to address other crimes e.g. theft, robbery, terrorism. As other MS did not provide similar statistic, the correlation can not be generalised.

The channels to forward requests and send replies differ not only between MS but also within a MS. In some MS, the interaction between operators and police (and other) authorities is centralised in both directions (f.i. a Single Point of Contact -SPOC- in the UK), in others in one direction (reply) only (f.i. ES), or not at all. Sometimes, (encrypted) electronic networks were established between law enforcement authorities and some of the largest national operators, whereas interaction with smaller operators deploys other means of communication. Some MS set up automated systems to respond to typical requests (CZ, NL). Apart from email and web interfaces, delivery by fax or paper is used (e.g. PL, BG, CY, LV) that allows to keep a written trace of the request.

---

4 See Article 72 TFEU

The Working Group of Article 29 of directive 95/46/EC[5] launched on 8 December 2008 a Joint Investigation Action on the implementation of the Data Retention Directive[6] that examines the respect of data protection requirements concerning the type of retained data, the security measures and prevention of abuse and the storage limit obligation. The results of this investigation are not yet published (see also chapter 2.III).

2. Conditions for retention and use: retention period - type of crimes – type of data - purpose of use

Many MS started applying the DRD rather recently (e.g. PT on 04 08 2009, IT on 15 12 2009, PL on 01 01 2010) in particular the internet part, although most had previous experience with the use of retained data. Early 2010, seven MS (AT, BE, GR, IE, LU, RO, SE) still had to adopt national legislation.

The average retention period is 12 months. Few MS (DE, LU, LT, SK; NL for internet data) apply a six months retention period, and some longer periods (e.g. LV, SI: 18 months, IE, IT: 24 months). No objective elements were found that could explain the choice of the retention period: neither the prevalence of certain forms of crime, the geography of MS, or (in-)efficiencies of a law enforcement organisation seem to support the choice. LEAs favour in general a longer retention period as this allows solving more crimes, whereas civil society and data protection plead for shorter periods to reduce the privacy impact.

The DRD does not define the term 'serious crimes' (Article 1(1)). Some MS consider these to be crimes that carry a minimum penalty of a maximum of five years imprisonment (e.g. DE, BG, CY) or lesser penalties (e.g. NL, FR: 1 year), whereas some leave it to the discretion of the judge who authorises the access (e.g. CZ, ES, MT, PL, LT). Further details see annex 5. No objective or MS specific elements could be identified to explain the difference.

MS' implementation laws do not seem to make reference to the conditions of Article 3 DRD: all the data in Article 5 DRD must be retained without exception, also when they were not previously retained. This could mean, but evidence is missing, that the national legislator considered that all data of Article 5 are always "generated of processed" in the sense of Article 3.
The terminology used in national laws to describe the data to be retained is not always identical to that of Article 5, and even if it is, interpretation seems to differ (see also chapter 2.III and IV). The Expert Group mentioned in Chapter 1 is, *inter alia*, addressing this issue.

Some MS introduced additional categories of data to be retained (e.g. subscriber bank data in BE), or use generic data categories that are further specified in executive acts (e.g. FR). DE brought services that hide the IP-address (anonymisers) under its law to ensure it has a "meaningful scope". The connection with Article 15(1) of the e-Privacy Directive[7] that can allow for such extensions, was not always clear (see also chapter 2.III).
Many MS reported that retained data can be accessed for purposes other than those mentioned in Article 1(1) DRD, f.i. to prevent crime[8], to maintain public order in the context of a terrorist threat, to find a missing person or to identify a dead body, to respond to emergency calls or to address cases of immanent danger (e.g. hostage taking, kidnapping), or for capital market supervision. Certain MS (f.i. UK) reported that a judge may order an operator to provide retained data in the context of civil litigations (f.i. copyright infringements). Other MS reported that use for other purposes is not allowed (e.g. BG, IT[9]). The evaluation did not establish that the deviation from the purpose of the DRD was based on the above-mentioned e-Privacy Directive. The cross-border impact of the departure from the Directive could not be validated either (cf. section 2.I.6).

---

5 Full title + OJ

6 See http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_17_03_09_en.pdf

7 Directive 2002/58/EC of the European Parliament and of the Council, concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L201/37 of 31.7.2002

8 Cfr Article 15(1) of the e-Privacy Directive (previous footnote) ; the connection with that Directive could not always be made

9 See under section 2.A.4. Cases *Peppermint and Techland*

3. Adequacy and law enforcement relevance of the data retained under the Articles 3 and 5 DRD

MS reported to be generally satisfied with the list of data list of Articles 3 and 5 DRD. Examples of cases are contained in annex 8. Retained data are in particular used to identify a target for real-time lawful interception of telephony. The increasing use of web-based application-level communication services implies an evolution towards different strategies to identify such targets.

In spite of their limited conclusive value, the statistics (see annex 6) support the conclusion that the relevance of data decreases significantly with their age: [70%] of all data are use within 0-3 months of their storage and [85%] within 0-6 months. For the added value of older data, only anecdotal evidence is available.

Suggestions were made to amend for instance Article 3 DRD by adding "unconnected (unsuccessful) calls", the "switch on/off" time of a mobile phone (LT: e.g. "*when a device falls into the water*"), or amending Article 5(1)(f)(1) DRD to require the retention of location labels of subsequent cells that process a roving mobile phone call. The DE DPA reported that operators do sometimes unjustly retain latter date, the NL DPA stated its national law orders this. Some MS stated that the retention of the activation of prepaid services mentioned in Article 5(1)(e)(2)(vi)DRD may no longer be relevant as cards are activated in factory before they are shipped to vending points (see also Part B below).

4. Obtaining data: type of requests - standardisation of interaction - time to reply

In some MS (e.g. FR) LEAs and operators drew up a detailed repository of pre-defined requests, whereas in others, like DE, the law stipulates the kind of requests that can LEA can make[10]. The majority of MS reported the typical requests they use in practice (f.i. the list of incoming and outgoing calls per number, IMEI-, and IMSI-related data, subscriber identification, known MAC/IP address linking it to a user, etc). Telephony-related requests prevail. Search parameters mostly include the object number (phone number, IMEI, IMSI, cell-ID, …) and dependent information.
Most MS did not (yet) adopt standards to regulate the interaction between public authorities and operators. Some, like ES, adopted the ETSI handover standard TS 102 657. DE reports that it also applies the relevant recommendations, and that some *Länder* use an electronic interface[11]. LT stated it intends establishing a standardised central data system accessible to all competent authorities. Others, like CZ, have included procedures in executive laws, or agreed with operators on models (e.g. FR).

Many MS report that operators must reply "without undue delay" (f.i. CZ, DE, FR, CY), which echoes the words of Article 8 DRD without more precise content. In some MS (f.i. BE), the law stipulates the time within which a operators must reply. Tools to enforce this condition vary.
In practice, answers are given in a few hours in urgent cases, or in normal cases in one to several days. Delays up to one month are reported as well. Some MS (e.g. PL) state not to set or enforce any timeframe.
Some MS, f.i. CZ, report that setting deadlines can be counter-productive, because it can delay the delivery of data even if they could be given faster.
NL reported that up-to-date subscriber data are stored in a central database that can be consulted by competent authorities (±3 mln queries/year) without judicial authorisation.

5. Cost and effectiveness: reimbursement plans - effectiveness of the use of retained data – human resource impact

The national plans for cost reimbursement vary widely. The majority of MS do not reimburse costs incurred by operators to retain and retrieve data, invoking *inter alia* the duty to assist police in solving crimes, or the counterpart of conducting a gainful business, or not binding law enforcement to budgetary considerations. Others (e.g. FR, DE, NL) cover certain operational costs (OPEX): FR and DE adopted tariff lists that enumerate the different actions that administrations can request and their corresponding remuneration. LT covers the costs for retention if public authorities request to retain data for more than 6 months. A smaller group of MS (e.g. UK, FI, CZ) reimburse moreover capital expenditure (CAPEX) to acquire the equipment necessary to retain and retrieve data.

---

10 See Article 100g of the Criminal Procedure Act

11 ETSI ES 201 671.TS 101 671 and TS 102 232-01

The amounts of reimbursement differ per MS and sometimes per operator in one MS, so as to take into account "positive side-effects for the business" (AT).
Some suggestions were made to increase cost-effectiveness, such as centralising retained data so as to avoid "hiring [...] communication channels" between LEAs and operators (LT).
Insufficient information is available to explain the differences.

Some MS make reimbursement dependent on the quality of information provided (e.g. AT). MS concerned report that reimbursement leads to better focussed, more successful requests.

All MS confirmed the effectiveness of the use of retained data: it does significantly assist the investigation and prosecution of crime, which would not even be possible in certain cases, e.g. cybercrime, privacy infringements, possible without retained data. Retained data are generally not exclusive evidence, but forms with other electronic (f.i. emails, spreadsheets, databases) or physical elements part of the totality of evidence before the court.

As a consequence, the evidential value of retained data must be assessed on a case-by-case basis in the light of all relevant factors of a case. No quantitative data could be provided to support the positive, qualitative assessment. Since law enforcement resources are limited, the fact that retained data are used, signify they were deemed relevant.
CZ f.i. reported that use of traffic and location data "became one of the basic investigating methods for all types of serious crimes".

The retention of data is considered proportionate if it has considerable law enforcement relevance. If CAPEX is reimbursed, for instance, such considerations determine which operators must and which must not retain data.
The use of retained data is proportionate if other, less intrusive measures of criminal procedure have failed. Some Member States (e.g. EE, FI) provided information about how they make this assessment.

6. cross-border requests: number – authorities involved – age of data – procedures – storage abroad

The number of cases where requests for retained data involved another MS (were made or received is as low as 0,01% (CZ) or 1% (FR) of the total number. Delays are generally (very) long (FR: 10 days average; 20 days for a request for identification). LT reported that in combination with a short retention period the delays cause data to be "no longer available", and states that longer retention "will strengthen international cooperation".
To speed up procedures, it was proposed to appoint contract points between public authorities and CPSs (f.i. CY, CZ), establish fact sheets per MS containing legal and technical means police avails of to obtain data from operators (CZ), or to standardise data collection (LT). Many MS have a central body that processes international requests (FR: OCLICTIC; UK: SOCA).
In almost all MS competent authorities request the relevant judicial authority or prosecutor to issue an MLA. The SIRENE/SISNET network is sometimes used as secure transmission channel. The bilateral meetings showed that very few MS are aware of the possibilities offered by Article 3(4) of Council Framework Decision 2006/960/JHA[12].

MS execute MLA requests free of charge on a basis of reciprocity, even if the requested MS reimburses OPEX costs, or must translate the request.

All MS reported they protect traffic and location data as personal data and to apply the appropriate protection (see also section I.1 *in fine*).

7. telecommunication authorities; tasks – economic/market effect – cooperation

The tasks of the relevant national authorities regarding the management of retained data differ per Member State. The telecommunication authorities share with other authorities (in particular DPAs, Ministries of Justice and Interior) the responsibility for the implementation of the DRD. Their tasks can include the

---

[12] OJ L ... of 28 December 2006

protection of traffic and location data, and of communication privacy at the operators' side, collecting the statistics mentioned in Article 10 DRD, or if applicable: deciding the modalities for and level of reimbursement. In general they do not collect data to assess the economic impact of data retention.

II. Parliament and civil society

1. effect on civil liberties

One respondent[13] stated that the DRD has "*catastrophic impacts*" on citizens and end-users, and mentions f.i. an increase of prices, restriction of competition and freedom, and a systemic lack of trust.
The Marper jurisprudence was mentioned to question the legality of the data retention *per se*[14], "*the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society*".
Another respondent[15] stressed that the right to respect for private life and correspondance also covers personal information relating to telephone, e-mail and internet usage, and that the retention of traffic and location data are an "exceptional measure" applicable only when the general principles of data protection, that of proportionality in particular, are respected. For that reason the list of data of Article 5 should be considered as a maximum, and that "serious crimes" and "electronic communications services" in Article 1(1) DRD and "competent authorities" in Article 8 DRD are properly defined.
The retention period is considered by respondents as failed harmonisation, and everything beyond one year "clearly disproportionate". Data retention would bring an end to the right of anonymity for everyday transactions.

2. offsetting the impact

Respondents stressed that the Directive failed to deliver on the harmonisation of national laws, and on redressing market distortions which was its main goal, but also on the reduction of crime or achieving higher rates of crime clarification. Having regard also to the serious impact on civil liberties, they recommend numerous actions at EU level.
One respondent suggests in the first place to abolish the DRD, and if not, to allow, MS to opt-out, to exclude non-commercial services, to fully reimburse incurred costs, or to substantially improve an up-to-date data security.
Another respondent recommends to unequivocally define the concepts "serious crimes", "data" and "services", to explicitly exclude the use of retained data in civil proceedings, to make clear that the list of Article 5 is the absolute maximum, to limit the retention period to six to twelve months, and to identify -f.i. in a public list- which operators are covered.

3. new technologies and proportionality of the DRD

One respondent rebuffed claims that changes in the use of ICT would require a change in attitude towards the confidentiality of human behaviour, dispelling anecdotal evidence and highlighting the lack of statistical data. Data about internet use and location should no longer be retained, and data and types of services referred to in the DRD should be unequivocally defined..

III. Data Protection Authorities

1. Competencies: investigating operators – complaints – audits

DPAs are competent to investigate the processing of retained personal data by operators. Some DPAs mentioned the complementary (e.g. DE, NL, SK) or exclusive (FI) supervisory role of telecommunication authorities. An investigation can be initiated on the basis of a complaint or of the DPA's own initiative, and can consist of official correspondence, but also lead to an *in-situ* audit. Many DPAs (e.g. CY, CZ, DE, LT, NL, PT, RO, SI, SK) reported they can also investigate data processing by public authorities. Almost all seem to be competent to conduct audits at the premises of operators, and in some MS (e.g. CY, MT) of public authorities. Some DPAs reported they has no powers to access retained data (LV) or limited audit powers (SK, and UK needs a judicial warrant). The UK DPA stressed the need for technical competencies.

---

13 European Digital Rights (EDRi) and Arbeitskreis Vorratsdatenspeicherung
14 ECHR, S and Marper *v* UK of 4 12 '08, cases 30562/04 and 30566/04, paragraph 116
15 ICRI-K.U. Leuven referring to the Copland v. UK , 3 April 2007, Application no 62617/00, par. 44

It was recalled that the DRD does not apply to closed (non public) ICT networks that make up the majority of LEA networks.

The IT DPA stated that it carried out a number of "in-depth inspections" on data-retention related issues further to "claims and reports". The main data protection issues that were addressed were the use of data for other purposes; measures to prevent unauthorised access; the number of staff authorised to access the data; and the availability of an audit trail. Other DPAs (e.g. DE) reported that they visited operators, or conducted investigations (e.g. RO).
Only FI reported a complaints-based case that was brought by a citizen to the telecom regulator.

2. Problems: legal – practical - other

Some DPAs reported problems with the implementation of the DRD in their MS. In general the need for "adequate and non-excessive" implementation was highlighted (f.i. CZ). The SI DPA mentioned that ambiguity exists about the providers that must retain data, and advocate "more technical guidance".
The IT DPA mentioned it does not receive the same statistical information as the Ministry; other DPAs (f.i. LT) do get it; the LV and PT DPAs compiles the national statistics. The IT and PT DPAs mentioned that the increased outsourcing of data retention operations requires that the responsibilities of each operator are clearly stated. FI reported unsolved practical challenges, the NL and SI DPA lack of precise definitions of the (scope of the) data to be retained, and the RO DPA failing uniform data management by operators.
CY reported that (some) operators were not yet able to retain data about "unsuccessful calls".
A number of DPAs mentioned the Joint Investigation Action (see section A.I.1) that revealed f.i. cases of flaws in data logging, and the retention of data beyond what is required by law (DE) as well as excess retention periods, and imperfect security measures (IT).
Some DPAs stated they have notified recommendations to improve processing of traffic data (LT), or sanctions (IT).

3. Extraterritoriality: exercise of competencies

Some DPAs (f.i. LT, IT) confirmed that data are stored in other States, and challenge effective supervision. The IT DPA stated that storage outside of the EU is of "special importance" here. Any approach should reconcile corporate organisation, law enforcement, data security, and the right to personal data protection. DPAs seem to hold the view that the national data protection law should apply to national data irrespective where they are stored.

4. case law

Apart from some decisions taken by DPAs, limited case law exists[16]. A SI court confirmed the right of access to retained personal data. Few *ex-officio* investigations were conducted outside of the action reported in section A.I.1. Some proceedings are underway (e.g. in DE on the obligation of operators to carry the costs of data retention).

IV. Private sector

1. length of storage period: impact of the DRD

The lack of harmonisation of the storage period of the data to be retained and of cost compensation is perceived as the main failure of the DRD: it affects competition, competitiveness, and precludes standardisation of product solutions. The five major trade associations[17] unanimously stated "[...] *data retention would be much more effective if operators were obliged to retain the same data in the same format and the same rules were applied for access and handover to that data to LEAs in all MS*". Operators observed that once a request for data was made, they can be held for longer that the maximum retention period.

Operators report that in most MS data can be retained for longer periods for commercial reasons (e.g. PL, UK, IE, LV), and public authorities can access in that extended period. In other MS (f.i. FR, DE, LT) LEAs

---

16 e.g. IT Constitutional Court 2006/372 of 14 .11.2006, and 81/1993 and 281/1998; C-; Cases *Peppermint & Techland* v. *Wind telecommunicazioni SpA; & - v. Telecom Italia SpA.* About the prohibition to use retained data for purposes other than fighting crime; RO Constitutional Court 1258/2009 of 8 October 2009 -constitutionality exception; DE Constitutional Court ruling of 2 March 2010.

17 ECTA, ETNO, EuroISPA, GSMA, Cable Europe

are not allowed to access data beyond the legal retention period. In general, however, the effect of the DRD was that operators had to retain more data and for a longer period.

2. extent and start of the legal obligation to retain data

Operators confirmed that in the majority of MS the obligation to retain data started rather late and applies indiscriminately (see also section 2.I.2). Substantial experience exists with regard to the retention of telephony data and serving requests of public authorities. Such can not be said about internet data.

3. costs: data security - time to answer – organisational adaptations – reimbursement

All operators seem to store data that is retained under the DRD in a different, sometimes duplicate database, to be able to expediently meet legal obligations.

The five major trade associations highlight that cost reimbursement is "*crucial*" from the perspective of industry, and of public policy: it provides a governance tool, and an incentive to be efficient, effective and proportionate.

They note that "*no adequate cost-benefit appraisal has been undertaken to ensure the proportionality of the measures*", which would be f.i. to stress harmonised retention of telephony data and not internet data.

One major operator[18] reported to have spend € 5.2 mln on implementation and € 3.7 mln/year on operations and maintenance costs to retain ca. 40 Tbyte/year, respond to 12.891 telephony data, and to 6.450 internet data requests. PL operators mentioned their CAPEX investment was between €300.000 and €4,4 mln. The main NL operator reported €4 mln CAPEX expenditure for the implementation of the telephony part, 60% of which were attributed to design costs (e.g. to prevent redundant storage), and €5 mln are the estimated costs for the implementation of the internet part. Annual OPEX is estimated at €4 mln. Cost drivers were in particular the obligation to answer to requests "without undue delay".

Information to assess opportunity costs or of benefits, if any, from the installation of data retention equipment was not available. These data would be relevant to bring out implicit costs or benefits for operators that are partly or fully reimbursed or for those that do not have to retain data. Respondents stated that reimbursement would function like a break on spurious or extensive requests. Moreover it would remove some of the market distortion that puts EU operators in a disadvantageous position compared to non-EU competitors; this is in particular the case for internet communications.

All operators confirmed that additional investments were required to retain data under the DRD, including to comply with data security requirements, although some report that some expenditure was made in the context of prior data retention obligations.
The absence of clear definitions about extent and scope of the retention obligation in the national law was sometimes mentioned as causing uncertainty as to the infrastructure to put in place (e.g. PL, NL). The three main CZ operators f.i. are reported to have set up dedicated units; annual costs range from 230.000 to 807.000 Euro and are "fully reimbursed"; some set up a 24/7 continuity system. A provider of integrated retention solutions reported that large numbers of small NL service providers and email net hosts set up data retention pool foundations that retain their data and replies to requests of LEAs, and allow them to comply with the DRD.

4. obligations: legal certainty

Perception of the precise scope of obligations differs sometimes between national operators (f.i. PL). The major CY operator reported that it adopted a holistic security management system based on ISO 27001 and 27002 (*information security management systems).* The prohibition to retain data more than once[19] is at odds with the obligation [often] imposed on network providers to retain all data, including those of service or virtual network providers who are also under the obligation to retain data.

5. Response: direct foreign requests - number of requests

---

18 Deutsche Telekom (figures for DE only)

19 Cf Recital 13 DRD

In general: foreign requests are channelled through competent national institutions, in particular those that execute rogatory letters. Foreign operators are in general not eligible for cost reimbursement even if national companies are.

6. economic effects: competition – investments - retail price

According to the five major Trade Associations, the DRD has a "*significant impact on industry*"; operators are facing "*substantial capital and operational costs*", that are "*enormous*" for smaller ones.

This assessment is confirmed by individual operators (e.g. PL) that report pressure on prices that are, however, more of less levelled out in a domestic context, and delaying or cancelling certain other investments.

Certain items seem to trigger high costs, f.i. storing data about unsuccessful call attempts (PL: €5 mln for one operator).

One CZ operator f.i. reports that cost effectiveness is "not relevant" as costs are reimbursed; others that it could be increased by centralisation (setting up a single point of contact). No impact on competition was felt yet, but as LEAs focus on large operators and reimburse them, this could "grant them important market advantage".

7. storing data abroad: occurrence – transfers

Information is scarce. Market efficiencies seem to drive centralisation, but security policies may lead to keeping data in the own MS. Fundamental legal questions (which law applies to the data? How do authorities exercise oversight? Is an MLA required to obtain data generated in another MS but stored on national territory?) have not been addressed. A pragmatic approach seems to prevail.

B. ENHANCING TRACEABILITY OF USERS OF COMMUNICATION SERVICES

I. Law enforcement issues

1. Existing national measures: existence – scope

The share of users of prepaid services as a part of the total varies: from ±20% (e.g. FI) to ±80% (e.g. PT). In some MS the registration of users of pre-paid cards is mandatory (DE, ES, IT, GR, SK, BG as from 1.1.'10; NO also requires registration). the modalities differ per MS. In ES f.i. operators had to set up a register, in IT vendors of cards report the identity of users to a public registrar.
LT and UK reported that f.i. information about refills of the pre-paid card user's account can be requested.
The NL DPA reports that location data analysis, and sometimes IMSI catchers are used to identify users of prepaid SIM cards.

2. Efficiency: results – added efficiency

The effectiveness of relevant measures could not be assessed because of the absence of information or statistics. In the bilateral meetings drawbacks were addressed, such as purchase of cards by third persons, roaming with foreign prepaid cards, and misuse of registered identities. SK reported that the obligation to keep records of users of subscribed services is "justified and necessary for effective fulfilment" of law enforcement tasks.

3. Costs for the private sector

No information was provided. DE (telecommunication regulator) states that a small price increase could be possible.

4. European measures: need – content – training

A large number of MS (f.i. PL, CY, LT) stated they would welcome EU measures to make registration the ID of users of prepaid services mandatory, and cross-border exchange of certain data; This would not only "greatly facilitate" addressing serious crime, but would also remove the need to use more intrusive investigate techniques (e.g. IMSI catcher, digital fingerprinting, i.e. communication pattern analysis, discrete observation).
Only some MS (f.i. CY) report specific training about obtaining and using mobile phone and internet data

5. Market impact of measures

ES reports that the impact will be nil "since all operators have the same obligation".

6. Monitoring and enforcement: case law – experiences

MS concerned reported that measures were taken recently and that experience is still lacking.

II. Parliament and civil society

1. effect of national measures on civil liberties – impact

Respondents highlighted the growing feeling of being under "constant surveillance", which would be aggravated by introducing mandatory registration prepaid cards. They also stressed the inherent ineffectiveness of such measure because they can be easily dodged, and would lead to a situation where law-abiding citizens would be monitored and criminals would remain undetected.

2. measures to offset the negative impact

As anonymity is perceived as a fundamental right of citizens and in a democratic society, anonymising services should not be penalised, and anonymity should remain as an option for citizens. Better international cooperation should allow to find "more effective measures" (unspecified) to fight criminals that make use of electronic communications.

III. Data Protection Authorities

1. Measures to enhance traceability: cases - observations

No information was provided about cases, if any, that were brought to the attention of DPAs.
The PT DPA questioned the efficacy of the DRD itself since without mandatory registration, as ±80% of PT users that use prepaid cards, would not be covered.
The NL DPA expressed concerns about alternative means of user identification.

2. Means to identify users of prepaid SIM cards

Mandatory registration exists in IT; the IT DPA reported that location data can be disclosed without the consent of subscriber for rescue operations, or for emergency calls services[20]. A holder of a prepaid SIM card can obtain traffic data about incoming calls if "indispensable" to safeguard his/her rights "in connection with criminal proceedings". Finally, to prevent that cards are registered under another person's name, operators must obtain the authorisation of a person who owns more than 4 cards. The NL DPA warned against identity theft or fraud.
The DE DPA stated that national measures give "no guarantee" that the ID of the person linked to the pre-paid card is authentic.

IV. Private sector

1. Identification of users of prepaid services: number – type of requests

Operators confirm the existence of mandatory registration of users in only a limited number of MS. Some voluntary registration schemes exist. In those cases consent of the person concerned is required when transferring data (e.g. PL). An IT operator stated it captures the personal data included in the ID that is submitted,

---

20 IT DPA decision of 19.12.2008; recital 36 & Article 10(1)(b) of Directive 2002/58/EC

2. **Methods: means to identify users – effectiveness in comparison to registered subscribers**

The reliability of voluntarily registered identities is limited (e.g. PL). The existence of alternative means to identify users of prepaid cards was mentioned, f.i. profiling when duly authorised..

3. Conclusions

On the basis of the evaluation[21], the following conclusions can be drawn and recommendations can be made:

DRD

-
-
-
-

PREPAID SERVICES

-
-

[21] conference 14/5/09, input DR expert group, replies to questionnaire and bilateral meetings)

Annex 1

List of abbreviations

COM = European Commission
DG JLS = DG Freedom, Security and Justice
DRD = Data Retention Directive
DPA = Data Protection Authority
ECtHR = European Court of Human Rights
ECHR = European Convention on Human Rights
ICT: Information and Communication Technologies
IP = Internet Protocol
ISP = Internet Service Provider
LEA = Law Enforcement Authority
MS = Member States

Terminology used in as far as different from the DRD

"Subscriber data" in this report denotes the relevant data of Article 5 relating to the subscriber of a telecommunication or internet service, of a registered user, as mentioned in Article 2(b) DRD.
"Law enforcement authorities" in this report denotes national police, customs, judicial authorities (public prosecutor, magistrates, judges), and other authorities competent and responsible for the application and enforcement of the law.

Country codes:

AT – Austria
BE – Belgium
BG – Bulgaria
CH – Switzerland
CZ – Czech Republic
CY – Cyprus
DE - Germany
DK – Denmark
EE – Estonia
EL – Greece
ES – Spain
FI – Finland
FR – France
HU – Hungary
IC – Iceland
IE – Ireland
IT – Italy
LI – Liechtenstein
LT – Lithuania
LU – Luxembourg
LV – Latvia
MT – Malta
NL – Netherlands
NO – Norway
PL – Poland
PT – Portugal
RO – Romania
SE – Sweden
SI – Slovenia

SK – Slovakia
UK – United Kingdom

Annex 2

CONCLUSIONS AND RECOMMENDATIONS

ANNEX 3

CONCLUSIONS OF THE CONFERENCE "TOWARDS THE EVALUATION OF THE DRD" OF 14 MAY 2009

Annex 4

QUESTIONNAIRE
WITH A VIEW TO TAKE STOCK OF THE OPERATION OF 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

v 30 09 2009

INTRODUCTION

- Scope of the questionnaire

This questionnaire seeks to gather information about all relevant aspects of the operation of the Data Retention Directive that will allow the Commission to understand its practical functioning in a manner that is as complete as possible. On that basis in particular, the Commission will draft the evaluation report mentioned in Article 14 of the Directive, which is due for 15 September 2010.

The questionnaire addresses each of the four groups of stakeholders concerned by the application of the Data Retention Directive (hereafter referred to as DRD or Directive): Member States, the private sector, Data Protection Authorities and the European Parliament, and contains a chapter for each of these stakeholders (see below under "stakeholders concerned" for more details).

Moreover, the Commission wants to use chapter 1 of the questionnaire as guideline for the discussions that it intends to organise with Member States and non-EU EEA States individually between the end of September and the end of November according to a time table to be agreed upon in the meeting of 10 September 2009.

The **first group** of questions aims at providing the European Commission with feedback necessary to assist it in the evaluation of the Directive further to its article 14.

Article 14 DRD states:

1. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party established under Article 29 of Directive 95/46/EC.

Pursuant to Article 10 DRD, Member States are obliged to ensure they provide the Commission on an annual basis with statistics on the retention of data. The data collection template was developed by the Experts' Group on Data Retention and was presented to Member States at their meeting of 22 January 2009 in Brussels.

The **input required to conduct the evaluation** draws from multiple sources: the statistics provided under Article 10 DRD, the assessment of technological progress and of the market impact, but also on law

enforcement specific information to establish whether the list of data mentioned in Article 5 and the length of the retention period in Article 6 are adequate and sufficient,

The **second set** of questions aims at obtaining feedback to carry out the analysis that was requested by the JHA Council at its meeting of 27 and 28 November 2008. In its Conclusions (**see annex**) the Council asked the Commission to evaluate the effectiveness of existing (non-) legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phones with prepaid SIM cards. The Member States undertook to "supply, at the request of the Commission, all relevant information on legislative and non-legislative measures or technical solutions implemented to identify users of communications media, and their degree of operational effectiveness". This questionnaire contains the specific requests from the Commission to obtain the relevant information.

The evaluation will therefore consist of two strands, namely, the assessment of
- the degree to which the Data Retention Directive is fit for purpose, i.e. to establish the extent to which the harmonisation of obligations on information service providers (hereafter referred to as ISPs) is able to ensure that data are available for the purpose of the investigation, detection and prosecution of serious crime, and
- the degree of effectiveness of national measures to trace the identity of users to combat the criminal misuse and anonymous use of electronic communications.

- Stakeholders concerned

The stakeholders that are concerned by these two sets of questions are the following
1. EU Member States and EEA States and in particular (). law enforcement authorities (Ministries of Interior, and of Justice) and (b). telecommunication authorities (Ministry of Telecommunication, National Regulatory Authorities) (concerning chapter 1 of the questionnaire)
2. European Parliament and Civil Society (concerning chapter 2 of the questionnaire)
3. National data protection authorities and the European Data Protection Supervisor (EDPS) (concerning chapter 3 of the questionnaire)
4. Private sector (communications service providers, comprising internet service providers, fixed and mobile telecommunication operators, network and cable operators, etc) (concerning chapter 4 of the questionnaire)

- Preparation of the questionnaire

The questionnaire was prepared by DG JLS and DG INFSO in particular on the basis of input received from the conference "Towards the Evaluation of the Data Retention Directive" of 14 May 2009. It was discussed for the first time by the Subgroup "Evaluation" of the Experts' Group on Data Retention on 9 September 2009 and presented to Member State representatives on 10 September 2009 in a meeting in the Secure Zone of DG JLS in Brussels. The Commission invited comments from the representatives to that meeting by 17 September 2009 with the drafting of the final questionnaire thereafter.
The current version takes account of the comments from (in alphabetical order:) Austria, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Latvia, Romania, Spain, Sweden, the United Kingdom, France.

The Subgroup "Evaluation" is composed in the same stakeholder groups as the Experts' Group on Data Retention. It has 2-3 representatives of Member States, Industry, Data Protection and the European Parliament.

The questionnaire will be the backbone of the evaluation process.

- Content of the questionnaire

The questionnaire consists of two types of questions: *qualitative questions* that examine the modalities of and conditions under which the Directive operates, and *quantitative questions* to gauge data volumes, financial, technological and legal impacts, and ratios between different aspects.

The Subgroup "Evaluation" was of the opinion that replying to the qualitative questions would require less time than providing quantitative data.

In the questionnaire indicates all questions that require a quantitative reply as follows: "[Quantitative Reply]". The other questions are qualitative questions by default.

- Time table for replying to the questionnaire

This version of the questionnaire was handed out to Member States during the meeting of 10 September 2009. The Commission invited Member States to give their views on the content and form of the questions until 17 September, in view of issuing a final questionnaire on thereafter.

According to the Subgroup "Evaluation" a period of eight weeks is a reasonable period to formulate answers to the quantitative questions, and a period of twelve weeks reasonable to gather information necessary to answer the quantitative questions.
On the basis of that assessment, the Commission would like to receive th first answers from each of the stakeholder groups within its own chapter (see before "stakeholders concerned") to the first type of questions by 15 November 2009, and the second type of questions (quantitative) by 15 December 2009.

Processing of confidential or classified information

Transparency rules can require that the Commission discloses information upon request, unless stakeholders identify all or some (explicitly identified) replies to the questionnaire as coming under one of the exceptions mentioned in Article 4 (1) or (2) of Regulation 1049/2001/EC as appropriate. The intention of the Commission is to use the replies solely for the purpose of the evaluation. .Aggregated or anonymized results can be included in the report and will not expose individual stakeholders, for instance to illustrate certain positions and statements contained in the evaluation report.
Replying to certain questions could entail the disclosure of confidential or classified information.
Respondents are requested **to indicate in their answer to the questionnaire** whether answers should be treated as confidential or as classified information (EU Confidential or EU Secret] and to **provide these answers separately** via the appropriate procedure.
The Commission shall ensure that within its organisation the information received shall receive a level of protection that is equivalent to the level of protection offered by measures applied to that information by the stakeholder concerned. Stakeholders are invited to mention such measures and forward information accordingly. Information identified as such will be kept in the Secure Zone and will only be accessible to persons that have the appropriate clearance.

Comments about data categories
The Data Retention Directive covers three types of operational data: 1. Data concerning fixed network telephony; 2. Data concerning mobile telephony and 3. Data concerning Internet access, Internet e-mail and Internet telephony.
The subgroup "Evaluation" of the Experts' Group on Data Retention is of the opinion that in case precise quantitative data can not (yet) be provided, it is easier to provide the ratio between the different categories of data, in particular since the ration between Internet data in comparison to telephony data is changing in favour of the first.

Comment with regard to technological development

Article 14 DRD requires that the evaluation takes into account "further developments in electronic communications technology".
The convergent market is moving beyond the technology that was available in 2004/2005 when the Directive was drafted.

New broadband type services delivered through 3G-GSM and WiFi enabled mobile handsets for instance have an impact on the ability to compare network events being generated on networks. All stakeholders are request to consider the impact of this and other developments on the application of the Directive.

Definition of "Request"

The Subgroup "Evaluation" noted that one "request" (cf Article 8 and 10(1) of the Directive and under 1.A.1 below) can concern several (many) "data". The number of requests can therefore be significantly smaller than the number of data that are transmitted. Depending on the context, the answer should refer to the total number of requests or of data that are provided.

Apart from quantitative indications that provide meaningful insight in for instance in the volume of the data processing or of the impact of the operation of the Directive on economic operators, a qualitative assessment is required to establish *inter alia* whether the list of data in Article 5 of the Directive or the retention period mentioned in Article 6 are relevant and effective to achieve the purpose of the Directive, namely to detect, investigate and prosecute serious crime. In order to support fact-finding on this matter, Member States in particular are invited to forward case studies or examples of prosecution cases where retained data have assisted investigations and prosecutions.

Throughout the first set of questions (on the evaluation of the Directive) the expression "country" is used to denote the fact that the addressees of the questionnaire are not only the EU Member States, but also non-EU EEA States.

1 QUESTIONS TO MEMBER STATES AND AND NON-EU EEA STATES

1.A Qualitative and quantitative aspects of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10,

1.A.1 Law enforcement issues

1.A.1.a Total number of requests that are issued by year to obtain data retained under the DRD **[Quantitative Reply]**

1.A.1.b Number/percentage of these requests that are generated by type of requesting authority: 1. police, 2. judicial, and 3. other authorities (please specify as relevant) **[Quantitative Reply]**

1.A.1.c The time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data, or if unavailable, the average age of the data that are requested, ? The answer to this question may already have been provided in the context of the statistics of Article 10 DRD. **[Quantitative Reply]**

1.A.1.d Which communication channels are used to exchange information between law enforcement authorities and service providers (e-mail, fax, secure network, or other channels)? If certain channels are required to be used, please provide information about the channels to be used

1.A.1.e Type of crimes

1.A.1.e.1 For what types of crime does the national law authorise the acquisition and use of retained data? Please provide a list of these crimes

1.A.1.e.2 What is the average age of the data that has been requested for the different types of crime mentioned under I.A.1.e.1 ? **[Quantitative Reply]**

1.A.1.e.3 Does the national law allow for or prohibit acquisistion of data from communications providers of data subservient of the Directive and/or related instruments for purposes other than the investigation, detection and prosecution of serious crime (e.g. copy right infringements). If so, please provide details about the alternative purpose(s) or laws prohibiting such acquisition.

1.A.1.e.4 Assessment of the data to be retained

1.A.1.e.5 Does the national law transposing the Data Retention Directive or a related instrument, require the retention of other categories of data in addition to the data contained in Article 5 of the Directive? If so, please provide details about the additional data as well as the instrument in which this obligation is enshrined.

1.A.1.e.6 Adequacy and law enforcement relevance of the data retained under Article 5 of the Data Retention Directive

Please indicate whether the data the service providers must retain under Article 5 of the Directive are relevant and sufficient from a law enforcement perspective, and mention which data either should be removed from the list of Article 5 where redundant or be added where relevant data is not yet retained.

Member States are invited to motivate their answer and provide examples of situations that demonstrate the redundancy or the law enforcement requirements.

1.A.1.f Details of the requests that are issued

1.A.1.f.1 The kind of information that service providers are requested to retrieve; Please provide information about typical search parameters (information selection criteria) contained in requests for the acquisition of retained data, e.g. listing of the communications made from or to a given phone number, or on certain date, or at a certain hour, or listing of all calls made from a certain location, or of all numbers used by an identified user.

1.A.1.f.2 Did your country standardise or seeking to standardise the format for the acquisition and disclosure of communications data between public authorities and communications service providers (for instance in service level agreements, or by making reference to relevant ETSI standards)? If so, please provide information about the standard (form or format) for requests, the message format, the technical modalities and/or interface.

1.A.1.g Details of the replies to the requests mentioned under I.A.1.g

1.A.1.h Does the national law governing the acquisition of communications data enable the public authority to specify the time period within which data must be disclosed, as referred to in the Directive as "without undue delay". If so:

1.A.1.h.1 Please provide examples of time frames enforceable within the context of national legislation or by service level agreements between competent authorities and communication providers.

1.A.1.h.2 What measures do competent authorities avail of to ensure the respect of the time period within which they request the reply to be given?

1.A.1.h.3 Where relevant, do competent authorities distinguish between time periods within which they require the disclosure of data by communication providers and the type of request or type of data they need? If so, please provide examples of such differentiation.

1.A.1.i Reimbursement of costs

1.A.1.i.1 Does your country reimburse CAPEX[22] and/or OPEX[23] incurred by service providers? If so, please provide information about the type of costs that are reimbursed, as well as about the modalities and amount or ratio of reimbursement

1.A.1.i.2 Does your country make the reimbursement of costs conditional on the respect of certain conditions, such as, for instance, guaranteeing a certain quality of service (request profiles, amount of requests to be handled, speed of retrieval)? If so, could you please provide information about the conditions that service providers have to meet and the link between reimbursement scheme.

1.A.1.j Effectiveness - What is the success rate of the use of retained data

1.A.1.j.1 Did the use of retained data assist in crimes being detected and/or prosecuted within the courts that otherwise would have failed? . It so, please provide examples [can entail Quantitative elements]

---

[22] CAPEX or CAPital EXpenditure, are expenditures creating future benefits. In concrete terms it is the cost of developing or providing non-consumable parts for the product or system, and may also include the cost of workers and facility expenses such as rent and utilities.

[23] OPEX or OPerational EXpenditure are operating costs or recurring expenses which are related to the operation of a business, or to the operation of a device, component, piece of equipment or facility.

1.A.1.j.2 *How much does the use of retained data cost in terms of deployment of Human Resources and acquisition & maintenance of dedicated equipment ? What are the typical cost drivers?* ***[Quantitative Reply]***

1.A.1.j.3 *How can cost-effectiveness of the acquisition and use of retained data be increased?* ***[entails quantitative elements]***

1.A.2 National and transnational requests and answers

1.A.2.a Within this questionnaire, a "transnational request" means a cross-border request for the acquisition of communications data between EU Member States and non-EU EEA States as appropriate where:

1.A.2.a.1 *law enforcement authorities from another county requests you to provide data retained by service providers within your country (the "incoming requests") and*

1.A.2.a.2 *requests initiated by your competent authorities for data held within another country's jurisdiction (the "outgoing requests").*

Having regard to the total number of requests mentioned under section 1.A.1.a:

1.A.1.a.1 *how many (a) incoming and how many (b) outgoing transnational requests are processed by your country on an annual basis. When possible, please differentiate between judicial co-operation and non-judicial cooperation* ***[Quantitative Replies]***

1.A.1.a.2 *what is the ratio between national and transnational requests (total number of transnational requests)?* ***[Quantitative Reply]***

1.A.1.b What is the average time to:

1.A.1.b.1 *receive an answer to an outgoing request, between the moment of issuing the request and the reception of the answer (see also A.A.2.f)? What are the elements (for instance: type of procedure) that determine the length of the procedure?* ***[Quantitative elements]***

1.A.1.b.2 *provide an answer to an incoming request, between the moment of reception of the request and the sending of the answer? What are the elements (for instance: type of procedure) that determine the length of the procedure?* ***[Quantitative elements]***

1.A.1.b.3 *Which strategies could be deployed to reduce the time it takes to answer an incoming request?*

1.A.1.c Which authority takes the decision in your country to issue a transnational request? Are all law enforcement authorities entitled to make or prompt to make a transnational request?

1.A.1.d Does your country have a central point that issues outgoing requests or receives incoming requests? If so, please provide details about these central points.

1.A.1.e Costs

1.A.1.e.1 *If your country reimburses OPEX (see 1.A.1.k) do you reimburse national service providers in the same way for replying to transnational requests? Do you or do you plan to ask other Member States to share the costs?*

1.A.1.f Language

1.A.1.f.1 *Does your country impose linguistic conditions to incoming requests (e.g. translation in a national or vehicular language? If so, please provide details about those conditions.*

1.A.1.f.2 *What means does your country deploy to comply with linguistic conditions imposed by other countries to outgoing requests? Do you have a central facility to provide linguistic support?*

1.A.1.g Data security

Which measures (rules, procedures, audit provisions) are enforced to protect data against misuse?

1.A.2 Telecommunications authorities

1.A.2.a Allocation of tasks

1.A.2.a.1 *Which national authorities are charged with tasks resulting from the Directive (for instance, as appropriate, following up with relevant service providers about applicable law, specifying content of data to be retained e.g. in CDRs, providing for a certain standardisation e.g. on the basis of ETSI standards, managing reimbursement schemes, assessing the economic impact of the implementation and application of the Directive)? Which tasks are assigned to which authority?*

1.A.2.a.2 *When did/will the respective authorities start to be operational for these tasks?*

1.A.2.a.3 *For each authority: Did/does the authority need to acquire additional expertise in order to perform its tasks under the Directive? Which? How was this implemented (e.g. new staff, reorganisation, special training) or how will it be implemented?*

1.A.2.a.4 *Does any authority mentioned under this section collect data about the economic effects of measures required under the Directive, including the impact of replying to court orders to provide retained data issued by Civil Courts on the request of copy right owners in cases brought by them against illicit downloading and file sharing of copy right protected material. If the answer to this question is affirmative, please provide details about the authority as well as about the data that are collected?* ***[May entail Quantitative elementsy]***

1.A.2.a.5 *Does any authority mentioned under this section engage in cross-border co-operation relating to the Directive? If so, please provide details about 1. those authorities 2. the type of action or activity that these authorities undertake in this context.* ***[may entail Quantitative elements]***

1.A.2.a.6 *Do the authorities mentioned under this section gather data concerning the impact of the required measures on competition e.g. on market entry for new operators, on advantages for bigger companies? Please provide details about the kind of data that are being collected!* ***[last par may entail Quantitative elements]***

1.A.2.a.7 ***Centralised storage of data by Service providers***

Does your country have problems (e.g. time to obtain an answer, quality of the reply) to obtain retained data that are stored by service providers outside of your country. Please provide details of problems you may have experienced and means deployed to redress these problems. **[can entail Quantitative elements]**

1.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards (cfr Council Conclusions in Annex)

1.B.1 Law enforcement issues

1.B.1.a Which means (technical, operational) or measures (procedural, law-based) does your country deploy to increase the traceability of users of communication services so as to assist law enforcement authorities in the attribution of end-user devices to the person using them? Among the measures mentioned are those that take account of data that are presently held by communication providers, such as customer service notes, payment history, insurance agreements, IMEI history, but also supermarket loyaly cards associated to the top-up history, use of e-top-up linked to debit or credit cards, information held by credit reference agencies and mobile device given as contact point, forensic examination of mobile devices? Please provide a description of these measures.

1.B.1.b What is the scope of these means or measures in terms of contribution to increasing the traceability of users ? Please provide details about the legal justification or administrative motivation and as well as about the scope of these instruments, i.e. whether they are aiming to assist the prevention of crime, or its detection, investigation or prosecution. Which crimes are specifically addressed by the means and measures that your country deploys..

1.B.1.c Efficiency

1.B.1.c.1 *Are the measures imposed by your country efficient in terms of achieving the aim for which they have been put in place? Please provide details about results obtained as a result of the deployment of the relevant means or measures* ***[may entail Quantitative elements].***

1.B.1.c.2 *Did your country assess the effectiveness of the measures If so, please provide details of this assessment.*

1.B.1.c.3 *What is the added efficiency of the measures deployed by your Member State in terms of improvement of your capabilities to detect, investigate or prosecute of terrorism and other serious forms of crime that go beyond the results obtained with the data obtained under Article 5(1)(e)(2) of the Directive and in particular its paragraph (vi)?* ***[can entail Quantitative elements]***

1.B.1.c.4 What are the costs or these measures for the private sector? ***[can entail Quantitative elements]***

1.B.1.d Should measures be taken at European level to increase the traceability of users of communication devices? If so, which measures should be taken, at European level? How would these measures improve the efficiency of the means and measures that you deploy at national level?

1.B.1.e Which training or skill-development scheme, if any, does your Member State provide for law enforcement authorities to train them in attributing (linking) end-user devices (e.g. mobile phones) to data that are held by communication providers to identify the end-users?

1.B.2 Telecommunications authorities

1.B.2.a *Which impacts on the market do the means or measures mentioned in section 1.B.1 have?*

1.B.2.b *Does the authority mentioned in 1.A.3.a.& monitor and enforce national measures on providers or other stakeholders?*

1.B.2.b.1 *Did the authority mentioned in the previous question investigate any cases of non-compliance with national means or measures? Please provide details, if relevente.* ***[can entail Quantitative elements]***

1.B.2.b.2 *If the national law provides for measures to ensure the identification of users of prepaid SIM cards, what treatment is given to the cards acquired before the entry into force of the law? Are these cards cancelled after a certain period in use?*

2 QUESTIONS ADDRESSED TO THE EUROPEAN PARLIAMENT AND CIVIL SOCIETY

2.A Assessment of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10

2.A.1 Which has been the effect, if any, on civil liberties of the use by law enforcement authorities of data retained under the Directive? Please provide examples of these effects as well as indications of the size of their impact.

2.A.2 What additional measures (administrative, technical, legal, or other) would be appropriate for the offset of any negative impact(s) which has been identified?

2.A.3 Which ones of the measures mentioned under 2.A.2 should be addressed at the level of the European Union?

2.A.4 Having regard to changes in technology and experience gathered with the operation of the Data Retention Directive, is the balance provided for by the Directive between enhancing security by means of retaining communication data and protecting civil liberties still appropriate . If a different balance is deemed to be appropriate , please provide details how to adjust the balance as well as the motivation underlying the assessment . **[can entail Quantitative elements]**

2.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure the traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards.

2.B.1 What has been the effect, if any, on civil liberties of measures taken at national level to increase the traceability of users of communication devices? Please provide examples of these effects as well as indications of the size of their impact.

2.B.2 Which additional measures (administrative, technical, legal, or other) should be taken for the offset of negative impacts, if any?

2.B.3 Which ones of these measures should be addressed at the level of the European Union?

3 QUESTIONS ADDRESSED TO NATIONAL SUPERVISORY AUTHORITIES AND THE EUROPEAN DATA PROTECTION SUPERVISOR (EDPS)

3.A Assessment of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10Please provide information on the distribution of competences of supervisory authorities according to Directives 95/46/EC, 2002/58/EC and 2006/24/EC.

3.A.1 Do authorities have investigative powers *vis-à-vis* providers? Which cases of complaints, if any, that have led to supervisory or investigative activities? Please provide for an overview of these activities and the outcome of proceedings.

3.A.2 Do authorities have investigative powers *vis-à-vis* public authorities? Which cases of complaints, if any, that have led to supervisory or investigative activities? Please provide for an overview of these activities and the outcome of proceedings.

3.A.3 Do authorities have the power to audit the compliance of providers and have there been any audits? If so, please provide details about such audits and the outcome of proceedings. **[can entail Quantitative elements]**

3.A.4 Which problems have supervisory authorities identified with the practical implementation of the Directive? (legal, practical, other; please provide details) **[can entail Quantitative elements]**

3.A.5 What experience do authorities have with the supervision of data that service providers have stored centrally, i.e. either within their jurisdiction or beyond? If so, please provide details about the challenges met in that context, also with regard to data stored outside of the EU/EEA. Please specify in particular the data protection issues that have been addressed that that context and the approach that has been followed to settle the contentious issues. [can entail Quantitative elements]

3.A.6 Please provide details about case law (jurisprudence), if any, with regard to the implementation or use of the Data Retention Directive or concerning the use of retained data within criminal investigations?

3.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards. Please provide details of the observations made by the data protection authorities with regard to practical needs and privacy issues surrounding measures intended to increase the traceability of users, if any, in particular of mobile pre-paid SIM cards, in particular from the point of view of ensuring the appropriate balance between the respect the privacy of users and security interests. In case any procedure has been brought against the such means or measures deployed in your country, please provider details about this procedure. *[can entail Quantitative elements]*

4 QUESTIONS TO THE PRIVATE SECTOR (ISPs, TELECOM OPERATORS, NETWORK AND CABLE OPERATORS)

4.A Assessment of the application of Directive 2006/24/EC, taking into account further developments in electronic communications technology and the statistics provided pursuant to Article 10.

For all questions in this section, please differentiate by type of service if applicable

1.A.1 Does the implementation of the Directive have the effect of requiring communication providers to retain data for a longer period than permitted for business purposes under Directive 2002/58/EC?

1.A.2 Do national authorities oblige communication providers to retain data, e.g. regardless of size, customer type and number, type of service? If national authorities differentiate between private sector stakeholders, please describe the criteria for .such differentiation.

1.A.3 Since when are data retention obligations in force, and, where relevant: since when is data retention applied in practice within a specific Member State with regard to specific communication providers?

1.A.4 Please provide details about the investment costs, if any, to fulfil their obligations on:

1.A.4.a retaining the data for the period required by national law,

1.A.4.b ensuring the security requirements imposed by the Directive,

1.A.4.c responding to requests without "undue delay", as defined by national law or in a service level agreement.

1.A.4.d ensuring that data are only retained for the purposes defined in the Directive and separated from data used for business operations, as determined by national law and necessary.

1.A.5 Please provide details about the implementation of specific organisational measures and procedures, if any, by communication providers that are necessary to comply with the obligations identified in the previous question (a-d)?

1.A.6 Is it possible to quantify financial impacts of the necessary measures? If so, please provide the relevant information to assess this impact. [can entail Quantitative elements]

1.A.7 Does the reimbursement by national authorities, if any, cover the expenditure necessary for compliance with the Directive?

1.A.8 Does the relevant legislation and practice provide providers with legal certainty regarding their obligations concerning the protection of data of their subscribers and users?

1.A.9 Have providers received direct requests from authorities in another Member State than that of their establishment? Were their any problems with these requests? If so, please provide for a description of these problems.

1.A.10 Please provide information, differentiated by type of operator etc concerning the elements of section 1.A.1 of this questionnaire.

1.A.11 Which economic effect do providers observe

1.A.11.a on competition,

1.A.11.b investment in new infrastructures and services,

1.A.11.c retail tariffs? Please provide quantitative information, and where such is not possible, qualitative indicators to allow assessment of the economic effect.

1.A.12 Centralised storage of retained data

1.A.12.a Do operators store data at a centralised level outside of the country where the data are generated? If so please provide details about the location, size and business impact of the centralised storage

1.A.12.b Do operators transfer retained data that are stored at centralised level to other countries that are bound by the Data Retention Directive or to third countries?

1.B Evaluation of the effectiveness of existing (non-)legislative measures or technical solutions to ensure traceability of users of communications services, in particular mobile phone lines, opened with prepaid SIM cards

1.B.1 Please provide information about the number of cases where communication providers been requested to identify users of pre-paid SIM cards?

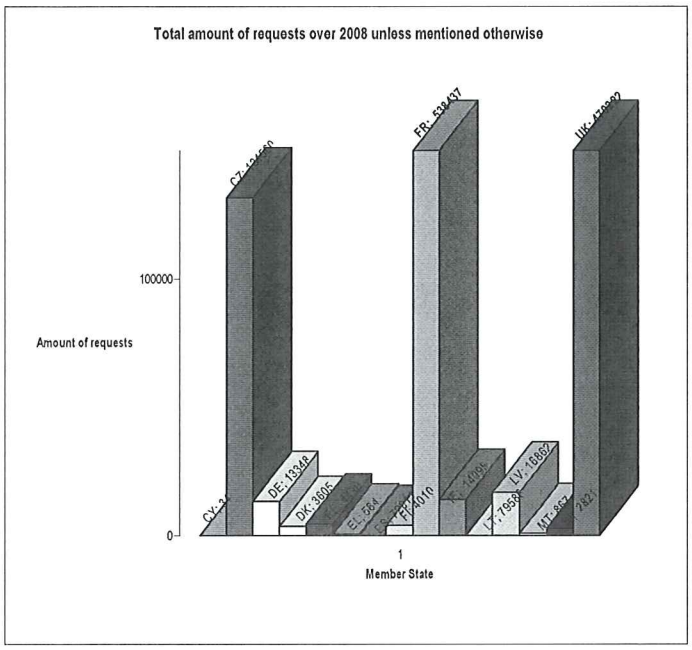
Which means do providers have to identify users of prepaid SIM cards? Please describe the number of cases or ratio of cases where information could not be provided in relation to the means used.

ANNEX 5

REPLIES TO THE QUESTIONNAIRE + SUMMARY OVERVIEW (KEY DATA)

STATISTICS

MS	Total amount of requests over 2008 unless mentioned otherwise
CY	34
CZ	131560
DE	13348
DK	3605
EE	4490
EL	584
ES	72011*
FI	4010
FR	538437
IE	14095
LT	79586**
LV	16862
MT	867
SI	2821
UK	470222



* : Statistics of ES show all requests "since 2007 until 2009"
** : Statistics of LT cover the period 03/09-11/09

Data Retention Directive - statistics 2008
Total Amount of Data that could be provided on Request
Aggregated on the basis of data from CY, CZ, DK, EE, IE, LT, LV, MT

	0-3 months	3-6 months	6-9 monthsc	9-12 months	12-15 months	15-18 months	18-21 months	21-24 months
Fixed communication data	12534	2220	1117	1467	136	158	23	16
Mobile communication data	117446	21556	9189	1109	491	322	66	43
Internet communication data[1]	1931	1047	731	1813	80	35	1	2

Data Retention Directive - statistics 2008
Total Amount of Data that could <u>not</u> be provided on Request
Aggregated on the basis of data from CY, CZ, DK, EE, IE, LT, LV, MT

	0-3 months	3-6 months	6-9 months	9-12 months	12-15 months	15-18 months	18-21 months	21-24 months
Fixed communication data	1373	1139	118	633	4	1	0	0
Mobile communication data	582	67	2303	39	16	1	2	1
Internet communication data[2]	67	101	102	54	0	3	0	0

---

[1] These data concern data on internet access, ~ telephony, and ~ e-mail

Annex 7

EVALUATION OF THE DATA RETENTION DIRECTIVE

Meetings September 2009 – January 2010

1 Bilateral meetings between the European Commission (DG JLS), Member States and EEA States

The bilateral meetings lasted for approximately three hours. They took place, at the discretion of Member States, with representatives of Member States in Brussels, or by video conference with capitals, in the Secure Zone or in an un-classified environment, with simultaneous interpretation or in a common language. The meetings and documents exchanged were classified or not.

The aim of this way of proceeding was to:
1. allow Member States and Commission to discuss all relevant issues without exception in relation to the operation of the DRD so as to give the Commission the fullest possible information to conduct the evaluation;
2. facilitate communication;
3. facilitate answering the questionnaire by clarifying its rationale and scope.

Date	Time	MS	Interpretation	Videoconference	Location
1. 29/09/2009	10:00 – 13:00	FR	No	No	DG JLS
2. 29/09/2009	14:00 – 17:00	UK	No	No	Secure Zone
3. 30/09/2009	14:00 – 17:00	DE	No	No	DG JLS
4. 01/10/2009	14:00 – 17:00	BG	Yes	No	Secure Zone
5. 07/10/2009	10:00 – 13:00	DK	No	No	DG JLS
6. 07/10/2009	14:30 – 17:30	ES	Yes	Yes	Secure Zone
7. 14/10/2009	14:00 – 17:00	EE	Yes	Yes	DG JLS
8. 15/10/2009	10:00 – 13:00	FI	No	No	DG JLS
9. 15/10/2009	14:00 – 17:00	GR	Yes	No	DG JLS
10. 19/10/2009	14:00 – 17:00	BE	No	No	DG JLS
11. 27/10/2009	14:30 – 17:30	LV	Yes	No	DG JLS
12. 04/11/2009	14:00 – 17:00	LU	No	No	DG JLS
13. 06/11/2009	14:30 – 17:30	CY	Yes	No	DG JLS
14. 12/11/2009	10:00 – 13:00	LT	No	Yes	Secure Zone
15. 12/11/2009	14:00 – 17:00	PT	Yes	No	DG JLS
16. 18/11/2009	14:30 – 17:30	RO	No	Yes	DG JLS
17. 19/11/2009	14:30 – 17:30	SK	Yes	No	DG JLS
18. 24/11/2009	10:00 – 13:00	MT	No	No	Secure Zone
19. 24/11/2009	14:00 – 17:00	AT	No	Yes	Secure Zone
20. 25/11/2009	14:30 – 17:30	HU	No	No	DG JLS
21. 26/11/2009	14:00 – 17:00	SI	No	No	DG JLS
22. 01/12/2009	14:00 – 17:00	IC	No	Yes	DG JLS
23. 02/12/2009	10:00 – 13:00	LI	No	Telephone conference	DG JLS
24/ 04/12/2009	10:00 – 13:00	SE	So	Yes	Secure Zone
25. 09/12/2009	14:00 – 17:00	NL	No	No	DG JLS
26. 10/12/2009	14.30 – 17:30	IE	No	Yes	Secure Zone
27. 14/12/2009	10:00 – 13:00	NO	No	Yes	Secure Zone
28. 14/12/2009	14:30 – 17:30	CZ	Yes	Yes	Secure Zone
29. 12/01/2010	10:00 – 13:00	PL	No	Yes	DG JLS

2. The Commission (DG JLS) had the following bilateral meetings with industries.

Date	Time	Company	Videoconference	Location
1. 05/11/2009	17:30 – 19:30	PRISM	No	DG JLS
2. 08/12/2009	12:30 – 15:00	Teradata	Including telephone conference	DG JLS
3. 14/01/2010	14:30 – 17:00	Deutsche Telekom	No	DG JLS
4. 25/01/2010	09:00 – 17:00	KPN Telecom	No	Rotterdam (NL)
5. 16/03/2010	12:30 – 14:30	Group2000	No	DG JLS

Council Conclusions on combating the criminal misuse and anonymous use of electronic communications

2908th JUSTICE and HOME AFFAIRS Council meeting
Brussels, 27-28 November 2008

The Council adopted the following conclusions:

"THE COUNCIL OF THE EUROPEAN UNION,

RECALLING the importance it attaches to the development in the territory of the European Union of electronic communications and of roaming, which are corollaries of the principle of the free movement of persons and of the establishment of a real "People's Europe";

WELCOMING the efforts of the European Commission, the Member States, national regulators and providers of electronic communications to improve communications between users, in particular through roaming agreements;

WELCOMING the reduction of roaming costs resulting from Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (the framework Directive) and Regulation (EC) No 717/2007 of the European Parliament and of the Council of 27 June 2007 on roaming on public mobile telephone networks within the Community and amending Directive 2002/21/EC;

RECALLING that the free movement of persons and the development of electronic communications must go hand in hand with the establishment of an area of freedom, security and justice, one of the substantive objectives of the European Union;

BEARING IN MIND 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) and Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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;

EMPHASISING the importance of the rules contained in the abovementioned instruments for both the protection of data derived from electronic communications and the conservation of such data for the purposes of criminal investigations;
DRAWING ATTENTION to the fact that organised criminal groups take advantage of the implementation of the principle of free movement of persons and the development of electronic (and especially mobile) communications to conduct their criminal activities in the territory of the Union;

NOTING that the impossibility, for the competent authorities, of identifying users of mobile telephones working with prepaid SIM cards can allow perpetrators of criminal offences to communicate with co-perpetrators or accomplices with complete impunity;

NOTING also that cross-border crime can be facilitated by the fact that, in roaming, the identity of the subscriber of the telephone line, registered with the home operator, is unknown to the host country operator registered in the destination country, whether that line operates on the basis of a subscription or a prepaid SIM card;

CONSIDERING the advantage there would be in being able to know the identity of the purchaser of a prepaid SIM card, in order to trace the user of a terminal;

EMPHASISING furthermore that mobile telephony is the medium of numerous criminal offences against mobile phone operators such as fraudulent reloading of prepaid phone cards and VAT fraud;

INSISTING that the development and intensification of police and judicial cooperation in criminal matters in European Union territory must be accompanied by improvements in the partnership between the public and the private sectors;

BEARING IN MIND its conclusions of 8 May 2003, in which it considered that the tracing of the use of prepaid mobile telephone cards could improve criminal investigations and particularly those relating to serious criminal offences,

CONCLUDES THAT IT IS NECESSARY TO COMBAT THE CRIMINAL MISUSE AND ANONYMOUS USE OF ELECTRONIC COMMUNICATIONS, AND TO THAT END:

RECALLS the importance of making the best possible use of the potential offered by the abovementioned European instruments;

INVITES Member States to supply, at the request of the Commission, all relevant information on legislative and non-legislative measures or technical solutions implemented to identify users of communications media, and their degree of operational effectiveness;

INVITES the Commission, in the context of the report referred to in Article 14 of the abovementioned Directive 2006/24/EC, and by 15 September 2010, to inform it of the legislative and non-legislative measures or technical solutions notified by the Member States and, on that basis, to propose non-legislative and technical solutions to help the services and authorities responsible for compliance with the law to better identify users of electronic communications services such as users of mobile phone lines opened with prepaid SIM cards and, if after evaluation it is apparent that these measures are unsuccessful in effectively ensuring traceability, to propose legislative measures;

SUGGESTS that these proposals also address the question of the reasonable retention period for information necessary to identify the phone user, given the time required for criminal investigations and in particular for those relating to serious forms of crime;

STRESSES that these proposals must take account of the objective of keeping the processing of personal data to a minimum and of using anonymous or pseudonymous data where possible, pursuant to the abovementioned Directive 2006/24/EC;

STATES that it is important that these proposals take account of their cost in relation to their anticipated benefit, and of a fair balance between the needs of the authorities and services responsible for criminal investigations and the economic development of operators and distributors bearing in mind the constraints which already weigh on them;

HOPES, finally, that the Commission proposals will, if appropriate, address any other difficulty encountered by Member States or their competent authorities in the framework of criminal investigations relating, in particular, to serious forms of crime, as regards the traceability of electronic communications, whether mobile or not – for example, difficulties relating to instant messaging used from a portable computer."

Annex 9

Anthology of cases involving the use of Retained Data

In the course of the bilateral meetings with MS some examples were discussed that illustrate the use of data retention as a crucial instrument for the fight against serious crime.

- CY reported that its police services were able to track an offender by acquiring mobile phone location data. The suspect first denied having been at the spot of the crime and having had any telephone conversations that could link him to the crime investigated. However, the retained data invalidated his alibi and linked him to the crime.

- HU report a serious case they could not have solved without the use of retained data. There has been a series of six killings. The murderers could be identified because of dial lists and the IMEI numbers of their mobile phones. The criminals tried to avoid detection by means of data retention by changing SIM cards. However, the IMEI numbers, which were also retained, demonstrated that the communications were made by the same mobile phone. The murders turned out to be hate crimes executed by extremists – all victims were Roma.

- LV had a case where a criminal was found guilty for having committed 17 robberies. At first, the police had difficulties tracing the criminal, because he used an anonymous prepaid SIM card. By studying the traffic data from this card, the police was able to trace the identity of the suspect's girlfriend and, as after further analysis, the identity of the suspect himself.

- MT police stated that it had been able to prevent people from committing suicide in several cases, thanks to data retention. People who had left a goodbye note or made a communication and who were determined to take their lives could be traced just in time by the police, who used the location data from their cell phones to find them alive.

- RO police services were looking for the identity of the user of a certain IP address. When they found out this IP address belonged to a hotel, they requested the hotel to provide information about the connection at a particular time.

- NO explained that it did not yet transpose the DRD, but that its police, duly authorised, can order operators to "freeze" communication data as from a given moment. The tool is, NO stated, rarely used as a tool for criminal investigation, since it is hard to identify the communication devices or user without availing of historical communications data. The NO police is therefore of the opinion that data freeze is not sufficient as an law enforcement instrument.

- UK reported once about Operation Backfill, concerning the investigation into a series of armed robberies where high value Audi motor cars were advertised for sale for "strictly cash only". The advertisements were posted on a website which specialised in the sale of used cars. When potential customers met up with the persons purporting to sell the cars they were held at gun point and demands made for their monies. The police commenced an investigation which examined the criminal's use of the internet. The investigators acquired internet related data (MAC address and consequential subscriber information) from the service provider which indicated the use of a lap top computer and premises from where the suspects had logged onto the internet when posting the advertisements. The suspects were arrested.