EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

Directorate F : Security
Unit F3 : Police co-operation and access to information

Brussels, 04/05/2010
JLS/F3/JV cn D (2010) 6751

Report of the meeting of Member States on Directive 2006/24/EC
(Data Retention Directive – DRD)
Brussels 12 March 2010
Conference Centre of the European Commission
Albert Borschette Room A0 AB

Absent: IT
Annex: room document: "Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of electronic communications"

Summary
The main purpose of the meeting was to elicit feedback on the representation of facts that were gathered by the Commission on the basis of input from Member States and (in some cases) Data Protection Authorities.
Few comments were made; many MS requested that the conclusions of the report were shared with MS prior to they being adopted;

1. Opening and welcome

On behalf of the European Commission, Ms Cecilia VERKLEIJ (DG JLS) welcomes participants. She briefly introduced the status and context of the evaluation of the Data Retention Directive. The intention of the Commission is to include the Directive in the Autumn Security Package to be presented to the JHA Council of 4-5 October 2010.

The agenda was adopted.

2. Adoption of the minutes of 23 November 2009

The minutes of the meeting of 23 November 2009 were adopted. Some MS had some final comments on the list in annex (status of the implementation of the DRD). They undertook to introduce these comments in writing until 17 March.

3. Presentation of the provisional findings of the evaluation of Directive 2006/24/EC (Data Retention Directive – DRD)

The Commission (Jacques VERRAES – DG JLS) presented the room document "Evaluation of Directive 2006/24/EC and of national measures to combat criminal misuse and anonymous use of

electronic communications" that contained a digest of the information that MS and other stakeholders had provided further to the questionnaire and bilateral meetings.

- *Infringement procedures and constitutional court proceedings*
The Commission briefed the Member States on the status of the implementation of the DRD. In that context, the infringements procedures that the Commission has brought against Member States (MS) that had not yet transposed the DRD were briefly mentioned. On 26 November the Court ruled on cases brought against IE (C-202/09), and GR (C-211/09), and on 4 February 2010 concerning SE (C-185/09). A case is pending against AT. AT mentioned that in spite of the fact that it had maintained in Court that the Directive violates fundamental rights, it remains committed to transposing the Directive.

DE and HU informed the other MS about the judgments of their national Constitutional Courts.

The RO Constitutional Court passed judgment on 8 October 2009 finding that Romania's national implementation of European Union's Data Retention Directive (Law 298/2008) violated Article 28 of the Constitution, pertaining to the secrecy of communication.
In February 2009, the Civil Society Commissariat (CSC) had filed a civil lawsuit against a telecommunications provider, seeking an order that would oblige it to honor its contracts which guarantee the confidentiality of phone conversations. The trial was suspended and the issue was brought to the Constitutional Court that ruled that in particular Article 28 was violated which reads "The secrecy of letters, telegrams, and other postal communications, of telephone conversations, and of any other legal means of communication is inviolable." The Court found that Law 298 was unconstitutional in its entirety because of its wide range of application and the positive obligation incumbent on all service providers to retain data; this leads to a permanent restriction of the right to privacy and the secrecy of correspondence, removing the essence of the right to privacy.
RO stated that at this moment, data are retained for the purpose of the detection, investigation and prosecution of crimes. It is currently examining under which conditions a new law can meet the ruling of 8 October as well as the obligations incumbent on it by virtue of the Directive.

The DE Constitutional Court gave its ruling on 2 March 2010 in which it found that the German law transposing the DRD is unconstitutional. As from that moment, no obligation or competence exists to retain data for law enforcement reasons. The Court found that data retention *per se* constitutes a serious interference with the private life of citizens whose communications and location data are being retained, in particular because of the "broad scope" of the retention obligation which goes beyond any existing law enforcement instrument. The Court considered that even though limited to communication traffic and location, the retained data allow drawing content-related conclusions.
The Court did not consider that the Directive itself was unconstitutional, as it leaves the national legislator a large margin of discretion to set up a national system for the access and use of stored data that takes account of the sensitive nature of data retention. The first attenuating factor mentioned by the Court was that data are distributed over a number of private service providers; this entails that operators lack the capacity to establish individual profiles, which require a combination of data. The second factor is that data storage is limited to six months "at the most". RO confirmed that its Court was of the same opinion.
The DE Constitutional Court stressing that the DRD does not cover access to or use of data, provided a number of precise conditions that the implementation law should include to make it constitutional, such as those relating to data security, the 4-eyes principle for accessing data, as well as logging, transparent control, limitation of use and the protection of the data subject in case of the use of data.

HU informed the meeting about the complaint that was filed on 26 May 2008 by the Hungarian

Civil Liberties Union requesting an ex post examination for unconstitutionality and the annulment of the Act on electronic communication that transposed the DRD into the Hungarian legal order which had entered into force on 15 March 2009. A hearing took place of the Ministers of Telecommunication on 12 December 2008 and of the Interior in May 2009. The ruling is not expected before the summer break.

FR highlighted that access and use presuppose retention, and that the purpose ("intention") for retention is not necessarily the same as the purpose for which the data will be used in the end. This is also true for the concept of 'serious crimes', which are, at any rate, left to the interpretative discretion of MS. At the moment data are retained or accessed, the exact nature of the crime is often not known. Other MS, however, (IE: 5 years; BU and LT: 6 years of imprisonment), reported that their police is under the obligation to access retained data only when it can be established *ex ante* that the crime to be addressed is a serious crime.

FR recalled that recital 25 of the DRD furthermore states that MS retain the power to adopt legislative measures concerning the right of access to and use of data by national authorities, which is an area that was covered by the Third Pillar under title VI of the TEU. Article 10 of the Transition Protocol to the Lisbon Treaty makes it clear that during the transition period (until 2014) the pre-Lisbon situation will be maintained in this area.

FR furthermore stated that one of the challenges for cross-border cooperation is to overcome the burdensome and time-consuming procedures for mutual legal assistance (MLA). The simplified procedure for obtaining judicial authorisation offered by Framework Decision 2006/960/JHA (simplifying the exchange of information and intelligence) cannot be used because access to the data requires coercing private entities to give data.

DE as well as AT requested the Commission to include in the evaluation an in-depth fundamental rights impact assessment against the EU Fundamental Rights Charter, and also to recall the arguments that were mentioned in the initial impact assessment which led to the conclusion that the DRD is compatible the Charter.
The assessment should allow determining *inter alia* which of the data falling under Article 3 and Article 5 of the DRD are the absolute minimums and which data are "not really necessary". AT suggested examining for which data the obligation to retain could be dropped, so that access to these data would only be possible during the period the data are retained for commercial purposes.
DE added that the evaluation should not only be based on an analysis of facts, but also take into account fundamental concepts, e.g. the fact that a 6 month retention period should be seen as the absolute maximum in view of the seriousness of the privacy infringement,.

AT recalled that subscriber data, such as name, address and bank details, are retained by providers also without legal obligation, to the extent that they are necessary for the business administration of a company, and are therefore of a different nature of traffic and location data.
The Commission confirmed that subscriber data remain under the ambit of Directive 95/46/EC (Data retention) whereas traffic and location data fall under the e-Privacy Directive.

- *Relation between Article 11 DRD and Article 15 of Directive 2002/58/EC (e-Privacy)*
In the context of the discussion about section A.1.1 'law enforcement issues" "national requests", a broad discussion took place about the extent to which the DRD depletes the margin that is left to Member States under Article 15 paragraph 1 of the e-Privacy Directive to enact national data retention legislation.

The Commission stated that the introduction of Article 15 paragraph 1(a) in Directive 2002/58/EC (e-Privacy) by Article 11 of the DRD read in conjunction with recital 12 of that Directive implies

that Article 15 "*continues to apply to data* [...] *the retention of which is not specifically required under* [the DRD] *and which therefore fall outside the scope thereof, and to the retention for purposes* [...] *other than those covered by* [the DRD]".

With regard to the limitation of the use of retained data for purposes other than those covered by the DRD, opinions diverge: in many MS retained data are used to prevent danger for life and limb, or to prevent crimes. With regard to the type of crimes that justify the use of retained data, the expression "serious crimes" in Article 1 is to be defined "by each Member State in its national law".
Further to a question by NL, the Commission clarifies that information society services (ISS) that do not qualify as electronic communications services[1] within the meaning of the definition in the Framework Directive 2002/21/EC (which is used in the ePrivacy Directive, e.g.. hotmail), are not covered by the e-Privacy Directive; as the DRD is an exception to the latter, it does not cover ISS either.

- *Statistics*
COM highlights the significant differences in the number of requests between Member States. Further examination of statistic reference and of the way statistics are collected should be undertaken.

UK mentioned that its national statistics include requests for subscriber data contrary to those of many other countries that only cover the access to traffic and location data. The initial impression that subscriber data are more often requested than traffic or location data requires further study.
UK requested to add more context to the statements in part "C" 'Statistics' about the fact that subscriber data are more often asked than traffic or location data.
In the first place, "subscriber data" encompass more elements than have to be retained on the basis of the DRD.
In the second place, the ratio between the number of requests for subscriber data and for other retained data changes over time as well as in relation to the context within which they are generated and used. For instance: the number of mobile phones per subscriber increases every year; in some Member States no national email providers exists or, due to the prevalence of flat rate billing, not much traffic data are generated.
Furthermore, the number of cases where law enforcement use internet-related data is significantly growing.

The low numbers of transnational requests was discussed. SE mentioned that due to the long duration of the process for requesting data abroad these data are often already deleted before the request arrives and is executed, which deters MS from asking such data in the future. CZ recommends "to find easier ways to handle requests", because currently "it takes days".

ES mentioned ongoing problems to generate national statistics. FI mentioned it will put a new handling system in place that will reduce the statistical granularity. SK stated that it considered the generation of statistics a "disproportional burden". HU mentioned it was developing a solution to be able to provide statistics.

NL states that the costs for transnational requests are, in particular, caused by the absence of hand-over standards.

Several delegations cautioned COM to use statistics parsimoniously and stay clear of strong

---

[1] Article 1 of Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society Services as amended by Directive 98/48 defines ISS as follows: *"any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services"*

conclusions.

- *Extraterritoriality*
Extraterritoriality of the application of national law poses a challenge because neither the retention period nor the conditions for access are harmonized. If an operator stores data outside the MS where the data were generated, conflicts are likely to occur.
FR highlighted the difficulties that operators run into when they have to manage the simultaneous application of different legal requirements to data in one database or within their company in one MS.

- *Data volumes - internet*
FR mentions that the volume of internet-related data to be retained under Article 5 is unwieldy; the reason is that the telephony data model (Mr A calls Mr B) was erroneously transplanted on internet leading to a cascade of mutually penetrating IP addresses that may or may not be spoofed by an anonymising service. Because processing of data occurs at different locations domestically and abroad, different laws apply to different datasets. FR states that it is necessary to clarify the situation.
SI added that in spite of the data volumes, the retention of IP address and E.164 calling number is not sufficient, inter alia because of the easy way to encrypt internet traffic. The current retention period (18 months) is "far too long" in the light of the existing political pressure.

- *Reimbursement; extent of the obligation to retain data*
FI stated that it continues to have a problem with the universal obligation on operators to retain data. As FI reimburses CAPEX, it is not able to subsidize all companies.
BE shared that it still had not decided.
IE stated that all-in-all the costs for the retention of data were modest considering that the telecommunication industry is a multibillion Euro industry.

- *Efficiency*
A number of delegations (e.g. UK, DK, PL) emphasized the unique opportunities provided to LEAs by the use of retained data.
DK stressed that the DRD is "a very useful tool and recommended to hold on to it and not to limit its scope". BG confirmed this point of view. SK stated it has "only positive references; the DRD helps us with our daily work".
PL stated it would like to include the obligation to retain the cell ID's of subsequent GSM base stations to keep track of a moving mobile phone. Commission explained that the DRD only provides for the retention of the cell ID at the beginning of a communication.

- *Further harmonisation*
In abstract terms delegations endorsed the idea that further harmonisation is appropriate. BG stated that lack of harmonisation is the root cause of deficient cross-border cooperation. Concrete issues where this harmonisation could be achieved were not identified during the discussion.

- enhancing the identification of users of prepaid SIM cards

FI, PL, and SE stated "there is no interest" in obliging users to register their identities. SI, RO, IE, DK, PL, CZ and UK reiterated that they were not in favour of imposing an obligation of users of pre-paid SIM cards to register them. Apart from opportunity crime that could be triggered by this registration, police avails of other techniques to establish the ID of anonymous users. It would also lead to public resentment. Besides, it would be easy to bypass any obligation which would annul the positive effect of that legislation. Some conceded that the only useful level of regulation would be

at EU level.

SK mentions that its current registration modalities are satisfactory; HU claims registration of users is "effective" and recommends legislation. ES and BU confirm the usefulness of mandatory registration. CY stated that prepaid cards are a "big problem" for the Cypriot police. BE stated that the law exists but that it has not yet been put into effect.

- *Final evaluation report and conclusions*
Some MS requested that all MS concerned by certain statements should be mentioned. COM stated that at many occasions, a reference to a MS was just to made in order to corroborate an assertion, and that the final report will only contain 22400 characters, i.e. about 30% less than the actual room document, accompanied by annexes with additional information.

Some MS (SE, FR, DE, ES, PT, UK, and HU) requested the Commission to share its conclusions with MS before submitting it for formal adoption by the Commission. The Commission stated, however, that the conclusions will have an important political component that does not allow having consultation going on in the margins.

4. Conclusions

Delegations were requested to provide their comments on the room document or on the annex of the minutes of 23 November 2009 in writing until 17 March. A new version will be circulated with these minutes.

Annexes:

- list of participants
- updated overview of the status of transposition of the DRD

Jacques Verraes

Annex to the report of the conference with Member States on 12 March 2010

Status of transposition of Directive 2006/24/EC
Reported by Member States and EFTA on 12 March 2010
based i.a. on oral communications during the meetings and written comments
[provisional version]

Country	state of implementation of Telephony	state of implementation of Internet	cost recovery issues	condition access & use of retained data
AT	law is under preparation by the government that was elected end 2008; the length and depth thereof could as of yet not be assessed.	law is under preparation by the government that was elected end 2008; the length and depth thereof could as of yet not be assessed.	One of the issues to be addressed: is the obligation of the government to reimburse costs incurred by CSPs	Request requires a court order; serious crime
BE	The law does already exist but still has to be brought in conformity with the DRD; the current retention period is 12-36 months; in the new law this will be brought to 24 months	idem	Study is carried out and will be published in 2010 on which basis it will be decided to reimburse or not	A request has to be made by an prosecutor or an investigating judge
BG	12 months retention period - national law is applied by means of Ministerial decrees since 15 09 2007	legal provisions should have been applied as from 15th March 2009 – but are still pending	no reimbursement of investment or operational costs	prosecutor with "passive technical access" to CSPs database based on a court order; Appeal against the order is possible; Mandatory registration of users of prepaid SIM cards;
CY	law entered into force on 1st January 2008 – retention period : 6 months	15th March 2009 the law entered into force – retention period 6 months	No reimbursement	Police must obtain a court order prior to requesting data to prevent, investigate and prosecute "felonies" and crimes punishable with imprisonment of > 5 years
CZ	Electronic Communications Act No. 127/2005 Coll. as amended by the Act amending Act No 127/2005 on electronic communications and amending certain related laws - No. 247/2008 Coll. – which entered into effect on September,1 2008. The Electronic Communications Act was followed by the DECREE No. 485/2005 Coll. on the extent of traffic and location data, the time of retention thereof and the form and method of the transmission thereof to bodies authorised to use such data.	Complete.	Government covers all (technical and service) costs incurred by service providers; estimated budget 4-6 million €.	Specific cases: 1. cases enumerated in the police act 2. The court on the basis of a Court order –Law of Criminal Procedure 3. National Bank in the remit of its mandate
DE	1st January 2008 case brought to the constitutional court against the law implementing the DRD – public	1st January 2009 idem	does not intend to reimburse investment costs; Grants "reasonable compensation" when requested to retrieve and transfer data; relevant law adopted; contains a range of flat indemnity rates; telecommunication providers have brought administrative action against the decision not to reimburse	Specific cases: 1. of considerable importance 2. committed using telecommunication means 3. necessary to establish the facts or determine the residence of the accused

Country	state of implementation of Telephony	state of implementation of Internet	cost recovery issues	condition access & use of retained data
	hearing on 15 December 2009 – judgement foreseen early 2010 On 2 March 2010 the Federal Constitutional Court declared the national implementation of the DRD unconstitutional		investment costs; does not provide financial support for the implementation	
DK	Implementation as of Sept 2007; (amendment of the Administration of Justice Act) – 12 months retention period	Idem – 12 months retention period	Only OPEX on the basis of an invoice issued by CSPs	DR pre-existed; Police can request when authorised by court order in a specific case of 'qualified suspicion' (excl. prevention) – pro forma lawyer defends interests of person whose data are accessed – scope: investigation of crimes carrying a punishment of at least a maxim 2 years imprisonment as well as certain specific crimes;
EE	Obligation to retain telephony data under the DRD applies since 2008 – retention period is 12 months	Obligation to retain internet data under the DRD applies since 15th March 2009 - retention period is 12 months	no cost reimbursement plan; costs of forwarding data are covered	DR pre-existed; Access be requested by law enforcement authorities; supervision process set up by the legislator; scope: investigation of crimes that carry at least a maximum penalty of three year imprisonment
ES	Law applies since May 2008 - law will eventually encompass ETSI TC 650 handover standard - format to be verified by the MoI and MoJ – retention period is 12 months	Law applies since May 2008 – retention period is 12 months	costs for the retention and retrieval are borne by providers – communication channel for providing retained data is paid by competent authorities	Access for serious crimes – officials of 7 authorities can request data – data must be delivered to central unit under each authority - court order required prior to requesting data – scope: concept of "serious crimes" subject of judicial interpretation - mandatory registration of users of prepaid SIM cards in force
FR	Law was adopted in 2007 – transposed by ministerial decrees 1. retention period 12 months - 2. DRD fully transpose d – case brought to the administra tive court was declared unjustified	idem	OPEX reimbursed according to tariff list	Judicial order required
FI	Retention of telephone traffic data applies as from June 2008 – 12 months retention period	Retention of internet traffic data applies as from 15th March 2009 – 12 months retention period	government reimburses CAPEX (telephony and internet) and OPEX for each transfer of data	To access traffic and location data: court order is required; to access subscriber data: can be directly obtained; access for "serious crimes", carrying at least an imprisonment of max. 4 years, as well as (attempted) offence "against a computer using a terminal device", pander, threatening a person to be heard by judicial authorities, menace, a drugs offence, preparation of a terrorist offence
GR	not yet transposed; draft law transposing the telephony part to be submitted to	2nd legislatory committee to be set up by new MoJ to draft the law transposing the	No reimbursement plan is foreseen under the current draft law	DR pre-existed ('05 Decree) ; specific order of publ. Prosecutor/judge is required -scope: investigation of serious crimes (incl preparation) - independent

Country	state of implementation of Telephony	state of implementation of Internet	cost recovery issues	condition access & use of retained data
	parliament; (retention period: [12] months)	internet part		authority exercises supervision – mandatory registration of users of prepaid SIM cards as from June 2010
HU	Since March 2009 the law entered into force in March 2008 – retention period 12 months and 6 months for unsuccessful call attempts	Idem	No cost reimbursement foreseen	
IE	Since 2005 – draft law transposing DRD pending – 5 stages : 2 year retention period	Legislative process is nearing its end; for implementation, IE could not give a firm deadline 1 year retention period retention period	no intention to reimburse costs incurred by providers – estimated costs CAPEX 2,5 mln / OPEX 1,5 mln/annually	Request by single authorized senior police or military authority; under supervision of a high court judge
IT	30th May 2008	30th May 2008	No generation of additional costs for operators; State does not provide financial support for the implementation	Access restricted; requires written request to court, court order; authorisation to police
LT	Amendment of the e-Communications law ; applies since 15 March 2009	internet part transposed by amendment of the e-Communications law; applies since 15th March 2009	No cost reimbursement scheme exists	Request of the authority
LU	since 2005	since 2005	No cost-reimbursement scheme exists.	Examining; case of investigation of "serious offence"; sample catalogue lists the relevant offences
LV	National law applies as from 2007 - 18 months retention period	National law applies as from 2007 - 18 months retention period	No cost reimbursement	DR pre-existed – a special individual request to operators based on a judicial authorisation is required; scope: prevention & investigation of 'crimes'; specialised units process requests; standard request form
MT	September 2008, law introduced the obligation to retain telephony data	September 2008, law introduced the obligation to retain internet traffic data	No introduction of general cost reimbursement scheme; certain expenditure covered on a case-by-case basis	be requested by police and courts, based on a written request or, in cases of imminent danger, by email or phone; "serious crime" punishable by imprisonment of at least 1 year.
NL	The law of 18 July 2009 amending the telecommunication law in conjunction with a Royal Decree entered into force in August 2009	The law of 18 July 2009 amending the telecommunication law in conjunction with a Royal Decree entered into force in August 2009	Investment costs are not reimbursed. A fixed rate reimbursement scheme exists for each transmission of data	public prosecutor can order CSPs; serious crimes
PT	17th July 2008 the transposition law was promulgated - In May 2009 regulation on the interaction between Service providers and public authorities using dedicated software	Idem	No reimbursement of CAPEX and OPEX	requires a court order; serious crime
RO	18th November 2008 – the transposition law was declared unconstitutional on 8 October 2009 – situation uncertain	15th March 2009 – law declared unconstitutional	Investment costs (infrastructure) reimbursed by means of fiscal deduction	judicial authorisation to request from prosecutor; "serious crime".
SE	currently working on drafting a bill; bill has yet to be submitted to Parliament	idem	Not yet dediced	Not yet decided
SK	Since April 2008	Since April 2008	No cost-compensation scheme exists; operators carry all costs	Only 'competent bodies', e.g. courts and secret service - police has direct access to a database with the

Country	state of implementation of Telephony	state of implementation of Internet	cost recovery issues	condition access & use of retained data
				identity of the users of fix and mobile telephony
SI	Transposed in Act of 12 Dec 2006 amending the Electronic Communication Act; obligation to retain data applies from 15 Sept 2007.	Transposed in Act of 12 Dec 2006 amending the Electronic Communication Act; obligation to retain data applies from 15 March 2009.	Cost-reimbursement is not provided under the Electronic Communications Act.	Retained data can be accessed on the basis of a court orde for the following purposes: - investigation, detection and prosecution of crimes stipulated in the Criminal Procedure Act (Art. 150); - for ensuring national security and the constitutional order, and security, political and economic interests of the state, as stipulated in the Slovene Intelligence and Security Agency Act (SOVA), - national defence as stipulated in the Defence Act Order of a competent authority is required. Who is the competent authority depends on the authority seeking access to the retained data; in majority of cases it is an investigating judge, but it could be also the Supreme Court or the director of SOVA.
UK	voluntary retention scheme is in place since 2004; obligation of retention of telephony data (fixed and mobile) exists since 2007	On 6th April 2009, the Data Retention (EC Directive) Regulations 2009 entered into force	reimbursement scheme covers capital costs of systems and staff; estimate d budget 30 million GBP/year	single point of contact processes requests; dedicated training available for officials entitled to request and access
EEA	postponed the implementation until Joint EEA-EU Committee has reached political agreement on the inclusion of the DRD into the EEA framework	idem	idem	idem