EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR HOME AFFAIRS

# Taking on the Data Retention Directive

Data Retention Conference,
3 December 2010, Brussels

**DISCUSSION PAPER FOR PARTICIPANTS**

## Background

Under Article 14 of the Data Retention Directive[1] (hereafter "Directive"), the European Commission was required to submit to the European Parliament and the Council no later than 15 September 2010 an evaluation of the application of this instrument and its impact on economic operators and consumers, taking into account further developments in electronic communication technology and the statistics provided to the Commission 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 [covered] and the periods of retention."

As the statistics provided by Member States proved insufficient for the completion of its evaluation report, the Commission requested a second round of data in the summer of 2010. This new information should enable the completion of this report by early 2011.

## Review of the Directive

The ongoing evaluation process and recent developments in various Member States have persuaded the Commission to consider a *broad* review of the provisions of this Directive, extending beyond data coverage and the length of retention periods.

Its internal reflection has focused on the following nine variables. Below the description of each variable, readers will find a number of questions for further discussion:

(1) **Purpose of data retention.** Data retention seeks to enable competent national authorities to investigate, detect and prosecute serious crime, as defined by each Member States in its national law. The e-Privacy Directive,[2] under Article 15, permits data retention for safeguarding national security, defence, public security and for preventing, investigating, detecting and prosecuting criminal offences or the unauthorised use of electronic communications systems.

---

1 Directive 2006/24/EC, OJ L 105, 13.4.2006, p. 54

2 Directive 2002/58/EC, OJ L 201, 31.7.2002, p. 37

- Does the expedited preservation of stored computer data[3] (known as 'data preservation' or 'quick freeze') pose a viable alternative to data retention?

- Are there any other viable alternatives to data retention besides data preservation?

- Should a potential new proposal on data retention have a broader purpose (similar to Article 15 of the e-Privacy Directive) or a narrower one?

(2) **Scope**. The Directive covers electronic communication traffic and location data, as well as information on subscribers and registered users. It expressly forbids the retention of data relating to the content of electronic communication.

- Should a potential new proposal include Information Society Services (ISS)?[4]

- Should the data on subscribers and registered users be treated the same way as traffic and location data?

(3) **Data retention period**. The Directive obliges Member States to ensure that data are retained for a minimum of six and a maximum of 24 months.

- Should the maximum retention period be different from 24 months?

- Should the minimum retention period be different from 6 months?

- Should there be a single retention period for all categories of data covered by a potential new proposal?

- Should there be different retention periods for mobile telephony, fixed telephony, internet data (including internet access, internet e-mail and internet telephony) and, if they are included in a new proposal, Information Society Services?

(4) **Definition of serious crime**. The Directive leaves it to Member States to define 'serious crime' to which retention obligations apply.

- Should a potential new proposal take the list of serious criminal offences set out in the European Arrest Warrant as the basis of its own definition?[5]

- Should a potential new proposal take the list of serious criminal offences set out in the Europol Decision as the basis of its own definition?[6]

---

3 Council of Europe Convention on Cybercrime [Article 16], Budapest, 21.XI.2001, ETS 185

4 Directive 98/34/EC, OJ L 24, 21.7.1998, p. 37

5 Council Decision 2002/584/JHA [Article 2(2)], OJ L 190, 18.7.2002, p. 1

6 Council Decision 2009/371/JHA [Annex], OJ L 121, 15.5.2009, p. 37

- Should a potential new proposal base its definition of serious crime on Article 83 of the Treaty on the Functioning of the European Union (TFEU)?[7]

- Should a potential new proposal develop its own definition of serious crime?

(5) **Authorities with access.** Under the Directive, competent national authorities may access retained data in specific cases and in accordance with national law.

- Should a potential new proposal specify the type(s) of national authorities with access to retained data?

(6) **Mode of access and cross-border transfer.** The Directive leaves it to Member States to define the procedures to be followed and the conditions to be fulfilled by competent authorities to gain access to retained data.

- Should a potential new proposal regulate access to and the cross-border transfer of retained data?

- Should a potential new proposal stipulate that an independent authority, such as a national contact point, shall receive, vet and authorise domestic access to and the cross-border transfer of retained data?

- Should it stipulate that a judicial authority shall authorise domestic access to and the cross-border transfer of retained data?

(7) **Operators under retention obligations.** Under the Directive, data retention obligations apply, within the jurisdiction of the Member State concerned, to the providers of publicly available electronic communication services or of public communication networks.

- Should a potential new proposal specify the operators under retention obligations?

- If yes, what criteria should inform the choice of operators under retention obligations?

(8) **Cost recovery.** The Directive contains no provisions on the potential recovery of costs incurred by operators in connection with data retention, yet several Member States have implemented such schemes.

- Should a potential new proposal contain a cost recovery scheme for operators under retention obligations?

---

7 Article 83, TFEU defines particularly serious crime with a cross-border nature as follows: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime.

- If yes, should such a scheme extend to capital and/or operational costs incurred in connection with data retention?

(9) **Data security**. The Directive sets out some basic provisions concerning data security.

- Should a potential new proposal specify in greater detail the data security obligations incumbent upon operators and authorities?

- Should it require the mandatory logging of users?

- Should it define a state-of-the-art data security regime similar to that included in the Prüm Decisions?[8]

European Commission, DG Home Affairs, October 2010

---

8 Council Decision 2008/615/JHA [Article 29], OJ L 210, 6.8.2008, p. 1; Council Decision 2008/616/JHA, OJ L 210, 6.8.2008, p. 12