



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 24 November 2005**

**14935/05**

**LIMITE**

**COPEN 187  
TELECOM 139**

**NOTE**

from :	Presidency
To :	Delegations
No. prev. doc. :	14328/05 COPEN 177 TELECOM 132
Subject :	Data retention

At the second trialogue meeting with the European Parliament on 22 November 2005, the representatives of the European Parliament emphasised that it was, from their perspective, of essential importance that the draft Directive on data retention contain:

1. provisions on access, whilst recognising the constraints to such a provision resulting from the limits of the legal basis for a Directive, and
2. a provision imposing criminal sanctions.

They also reiterated the need for additional data protection safeguards.

As delegations will be aware, the LIBE Committee voted through its formal position today. Though the Parliament's willingness and co-operation to hasten the process has been encouraging, there are still divergent views on several key issues between the institutions, notably retention periods, costs and scope of application. The report adopted by the LIBE Committee is of course the first step in the parliamentary process and negotiations will continue with the European Parliament in advance of the plenary meeting on 13-14 December.

With a view to securing a mutually acceptable outcome at that meeting, the Presidency asks COREPER to agree the attached as the basis for further negotiations.

---

**I Additional recitals:**

- (15bis) It should also be recalled that the obligations incumbent on service providers concerning measures to ensure data quality which derive from Article 6 of Directive 95/46/EC as well as their obligations [...] concerning measures to ensure confidentiality and security [...] or processing of data which derive from Articles 16 and 17 of Directive 95/46/EC, are fully applicable to [...] data being retained within the meaning of the present Directive.
- (16bis) In this context, it should be recalled that Article 24 of Directive 95/46/EC imposes an obligation on Member States to sanction infringements of the provisions adopted pursuant to Directive 95/46/EC; Article 15(2) of Directive 2002/58 imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58; Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems provides that the intentional illegal access to information systems, including to [...] data retained therein, shall be made punishable as a criminal offence.
- (16ter) It should be borne in mind that the right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC, to receive compensation [...], which derives from Article 23 of Directive 95/46/EC, applies also in relation to the unlawful processing of any personal data [...] pursuant to the present Directive.
- (17bis) It should be borne in mind that the 2001 Council of Europe Convention on Cybercrime as well as the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [...] also cover data being retained within the meaning of the present Directive.

- (Z) Issues of access to data retained pursuant to this Directive by national public authorities for such activities as are referred to in Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be the subject of national law, or action pursuant to Title VI of the Treaty on European Union, always noting that such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as they are guaranteed by the ECHR, as interpreted by the European Court of Human Rights. Case-law on Article 8 ECHR requires that interference by public authorities with privacy rights must respond to requirements of necessity and proportionality and must therefore serve specified, explicit and legitimate purposes and be exercised in a manner which is adequate, relevant and not excessive in relation to the purposed of the interference.

## II Additional provisions in the text:

### *Article 3*

#### **Obligation to retain data**

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation [...]. The process to be followed and the conditions to be fulfilled in order to get access to retained data and to preserve accessed data in accordance with necessity and proportionality requirements shall be defined by each Member State in national law, subject to relevant provisions of Union law or public international law.<sup>1</sup> Such provisions of public international law include in particular the European Convention on Human Rights, as interpreted by the European Court of Human Rights.

---

<sup>1</sup> The last sentence is based on Article 6 paragraph 2 of the draft Framework Decision.

### *Article 7bis*

#### **Data protection and data security**

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with the present Directive:

- (a) the retained data shall be of the same quality and shall be subject to the same security and protection as those data on the network;
- (b) the data shall be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, or accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;
- (c) the data shall be subject to appropriate technical and organisational measures to ensure that access to the data is undertaken only by specially authorised personnel;
- (d) that providers undertake regular and systematic self-auditing to ensure that the applicable rules on data protection are respected; and
- (e) the data shall be destroyed at the end of the period for retention except those data which have been accessed and preserved.

### *Article 8bis*

#### **Supervisory authority**

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive regarding the security of the stored data.
2. These authorities shall act with complete independence in exercising the functions referred to in paragraph 1. ]

**Remedies, liability and sanctions**

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.
2. Each Member State shall in particular take the necessary measures to ensure that intentional access to or transfer of data retained in accordance with the present Directive which is not authorised by the provider of publicly available electronic communication services or of the public communications network responsible for retention, or which is not permitted under national law, shall be punishable by sanctions, including administrative or criminal sanctions<sup>1</sup>, which are effective, proportionate and dissuasive.

---

---

<sup>1</sup> Precedent can be found in EC Regulations 2241/87 and 2847/93.