



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 14 October 2004

13353/04

**COPEN 122
TELECOM 150**

NOTE

from : Presidency

to : Working Party on cooperation in criminal matters

No. prev. doc. : 10841/04 CRIMORG 79 TELECOM 126

Subject : Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism

The Presidency has established the attached revised version of the above Framework Decision for the purpose of further proceedings in the Working Party on cooperation in criminal matters. The text has been established in the light of the discussions at the meeting of the Working Party on 27 and 28 September 2004, and having in mind also the proceedings in the Workshop of the Commission on traffic data retention on 21 September 2004 and the exchange of views on the draft in the Article 36 Committee at its meeting on 7 and 8 October 2004. Changes compared with 10841/04 CRIMORG 79 TELECOM 126 are indicated.

Draft Framework Decision

on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.

THE COUNCIL OF THE EUROPEAN UNION¹

Having regard to the Treaty on European Union, and in particular Article 31(1)(c) and Article 34 (2)(b) thereof,

Having regard to the initiative of the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom,²

Having regard to the Opinion of the European Parliament,

Whereas:

1. Offering a high level of protection in an area of liberty, security and justice requires that the prevention, investigation, detection and prosecution of crime and criminal offences be carried out in an adequate manner

¹ The preamble has not been examined.

² 8958/04 CRIMORG 36 TELECOM 82, not yet published and not yet submitted to the European Parliament.

2. The plan of action of the Council and the Commission on the best ways to implement the provisions of the Treaty of Amsterdam on the establishment of an area of liberty, security and justice, the conclusions of the European Council at Tampere on 15-16 October 1999, the European Council at Santa Maria da Feira on 19-20 June 2000, the European Commission in its scoreboard and the European Parliament in its resolution of 19 May 2000 call for an intervention in the area of high tech crime.
3. The conclusions of the Council of 20 September 2001 call for care to be taken to ensure that the forces of law and order are able to investigate criminal acts which involve the use of electronic communications systems and to take measures against the perpetrators of these crimes, while maintaining a balance between the protection of personal data and the needs of the law and order authorities to have access to data for criminal investigation purposes. It is noted in the conclusions of the Council of 19 December 2002 that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications is now a particularly important and valuable tool in the prevention, investigation, detection and prosecution of crime and criminal offences, in particular organised crime and terrorism.
4. The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers with a view to adoption by June 2005.
5. It is essential to retain data existing on public communications networks, generated in consequence of a communication, hereafter referred to as data, for the prevention, investigation, detection and prosecution of crimes and criminal offences involving the use of electronic communications systems. This Framework Decision relates only to data generated as a consequence of a communication and does not relate to data that is the content of the information communicated. In particular, it is necessary to retain data in order to trace the source of illegal content such as child pornography and racist and xenophobic material; the source of attacks against information systems; and to identify those involved in using electronic communications networks for the purpose of organised crime and terrorism.

6. Preservation of specific data relating to specified individuals in specific cases is not sufficient to meet these requirements. In investigations, it may not be possible to identify the data required or the individual involved until many months or years after the original communication. It is therefore necessary to retain certain types of data, which are already processed and stored for billing, commercial or any other legitimate purposes, for a certain additional period of time in anticipation that they might be required for a future criminal investigation or judicial proceedings. This Framework Decision therefore concerns the retention of data and does not relate to the preservation of data.
7. In recognition of the importance of the need to retain data, Article 15 of Directive 2002/58/EC permits the adoption of legislative measures allowing, under certain conditions, retention of data for the purposes of the prevention, investigation, detection or prosecution of crime and criminal offences. This framework decision is not related to other objectives set out in Article 15 of this Directive and therefore does not provide for rules on data retention for the purpose of safeguarding national security (i.e. State Security), defence, public security. Nor is it related to the unauthorised use of the electronic communication system when such use does not constitute a criminal offence.
8. Many Member States have passed legislation concerning a priori retention of data for the purposes of prevention, investigation, detection or prosecution of crime and criminal offences. Work in this area is under way in other Member States. The content of this legislation varies considerably between Member States.

9. The differences between the legislation in Member States is prejudicial to co-operation between the competent authorities in the prevention, investigation, detection and prosecution of crime and criminal offences. To ensure effective police and judicial co-operation in criminal matters, it is therefore necessary to ensure that all Member States take the necessary steps to retain certain types of data for a length of time within set parameters for the purposes of preventing, investigating, detecting and prosecuting crime and criminal offences including terrorism. Such data should be available to other member states in accordance with the instruments on judicial co-operation in criminal matters adopted under Title VI of the Treaty on European Union. This should also include instruments which were not adopted under this Title but which has been acceded to by the member states and to which reference are made in the instruments on judicial co-operation in criminal matters adopted under Title VI of the Treaty on European Union.
10. Such a priori retention of data and access to this data may constitute an interference in the private life of the individual. However, such an interference does not violate the international rules applicable with regard to the right to respect to privacy and the handling of personal data contained, in particular, in the European Convention on the Protection of Human Rights of 4 November 1950, the Convention of the Council of Europe no.108 on the protection of persons in respect of the automated handling of personal data of 28 January 1981, and the Directives 95/46/EC, 97/66/EC and 2002/58 EC where such interference is provided for by law and where it is appropriate, strictly proportionate to the intended purpose and necessary within a democratic society, and subject to adequate safeguards for the prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.
11. Taking into account both the need to ensure that data is retained a priori in an efficient and harmonised way and the need to allow Member States ample room to make their own individual assessments given the differences that exist between criminal justice systems, it is appropriate to establish parameters for the a priori retention of data.

12. Data may be a priori retained for different periods of time depending on its type. The retention periods for each type of data will be dependant on the usefulness of the data in relation to the prevention, investigation, detection, and prosecution of crime and criminal offences and the cost of retaining the data. The retention periods shall be proportionate in view of the needs for such data for the purposes of preventing, investigating, detecting and prosecuting crime and criminal offences as against the intrusion into privacy that such retention will entail from disclosure of that retained data.
13. The drawing up of any lists of the types of data to be retained must reflect a balance between the benefit to the prevention, investigation, detection, and prosecution of crime and criminal offences of keeping each type of data against the level of invasion of privacy which will result.
14. The Framework Decision does not apply to access to data at the time of transmission, that is by the monitoring, interception or recording of telecommunications.
15. Member States must ensure that access to retained data takes account of privacy rules as defined in international law applicable to the protection of personal data.
16. Member States shall ensure that implementation of the Framework Decision involves appropriate consultation with the Industry.

HAS ADOPTED THE PRESENT FRAMEWORK DECISION:

Article 1

Scope and Aim

1. This Framework Decision aims to facilitate judicial co-operation in criminal matters by approximating Member States' legislation on the continued¹ retention of data processed and stored by providers of a publicly available electronic communications service or a public communications network, for the purpose of (...)², investigation, detection and prosecution of terrorist and other serious criminal offences.

1a.³ This Framework Decision shall apply to all means of electronic communication, including in particular:

(a) Telephony excluding Short Message Services, Electronic Media Services and Multi Media Messaging Services.

(b) Short Message Services, Electronic Media Services and Multi Media Messaging Services provided as part of any telephony service.

(c) Internet Protocols including Email, Voice over Internet Protocols, world wide web, file transfer protocols, network transfer protocols, hyper text transfer protocols, voice over broadband and subsets of Internet Protocols numbers - network address translation data.

¹ The Presidency proposes to add the term "continued".

² The reference to "prevention" has been deleted in connection with the deletion of Article 1(3) and the addition of the first indent of Article 3(4).

³ The text of Article 1(1a)(a), (b) and (c) corresponds to former Article 2(3)(a), (b) and (c). The "chapeau" is re-worded so that it covers the substance of former Article 2(4).

2. This Framework Decision shall not apply to the content of exchanged communications, including information consulted using an electronic communications network.
3. (...)
4. This Framework Decision is without prejudice to:
 - national rules on retention of data (processed and stored by providers of a publicly available electronic communications service or a public communications network) for the purpose of prevention of crime;
 - the rules applicable to judicial co-operation in criminal matters with regard to the interception and recording of telecommunications;
 - activities concerning public security, defence and national security (i.e. State security);
 - national rules relating to the retention of data types which are not held by communication service providers for business purposes.

Article 2

Definitions

1. For the purpose of this Framework Decision:
 - (a) The definition of the term ‘data’ in this Framework Decision means traffic data and location data as set out in Article 2 of the Directive 2002/58/EC, and (...) subscriber data and user data related to these data.

(b) User data means data relating to any (...) person¹ using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to the service.

(c) Subscriber data means data relating to any (...) person² subscribing to a publicly available electronic communications service for, private or business purposes, without necessarily having used the service.

2. Data includes in particular:

(a) Data necessary to trace and identify the source of a communication which includes personal details, contact information and information identifying services subscribed to.

(b) Data necessary to identify the routing and destination of a communication.

(c) Data necessary to identify the time and date and duration of a communication.

(d) Data necessary to identify the telecommunication.

(e) Data necessary to identify the communication device or what purports to be the device.

(f) Data necessary to identify the location at the start and throughout the duration of the communication.

3. (...) ³

4. (...) ⁴

¹ The reference to "persons" includes natural as well as legal persons.

² The reference to "persons" includes natural as well as legal persons.

³ See footnote 2 on page 7.

⁴ See footnote 2 on page 7.

Article 3

Retention of data

Each Member State shall take the necessary measures to ensure that, for the purpose of providing judicial co-operation in criminal matters, (...) data processed and stored for billing, commercial or any other legitimate purposes by providers of a public communications network or publicly available electronic communications services (...) is retained in accordance with the provisions of this Framework Decision (...).

Article 4

Time periods for retention of data

1. Each Member State shall take the necessary measures to ensure that stored data referred to in Article 3 shall be retained for a period of 12 months following its generation. Relating to subscriber data, this period shall run from the end of the subscription.
2. Member States may have longer periods for retention of data dependent upon national criteria when such retention constitutes a necessary, appropriate and proportionate measure within a democratic society.
3. A Member State may allow shorter periods of retention for data types covered by Article 2(2) in relation to means of communication identified in Article 1(1a)(b)¹ and (c) should the Member State not find acceptable, following national procedural or consultative processes, the retention periods set out in paragraph 1 of this Article.

¹ The Presidency invites the Working Party to consider whether the reference to Article 1(1a)(b) should be retained.

4. A Member State deciding to make use of paragraph 3 at any time must give notice to the Council and to the Commission stating the alternative time scales being adopted for the data types affected. Any such derogation must be reviewed annually.¹

Article 5

(...)²

*Article 6*³

Data Protection

Each Member State shall ensure that data retained under this Framework Decision shall be subject, as a minimum, to the following data protection principles and shall establish judicial remedies in line with the provisions of Chapter III on 'Judicial remedies, liability and sanctions' of Directive 95/46/EC:

- (a) data shall be accessed for specified, explicit and legitimate purposes by competent authorities on a case by case basis in accordance with national law and not further processed in a way incompatible with those purposes;
- (b) the data shall be adequate, relevant and not excessive in relation to the purposes for which they are accessed. Data shall be processed fairly and lawfully;
- (c) data accessed by competent authorities shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the data were collected or for which they are further processed;

¹ This paragraph was originally the last sentence of paragraph 3 of this Article.

² Article 5 has been deleted. The access to data retained in accordance with the Framework Decision is thereby, with the exception of Articles 6 and 7, regulated by provisions outside the Framework Decision, for example as mutual legal assistance provisions.

³ Articles 6 and 7 need further consideration.

- (d) the confidentiality and integrity of the data shall be ensured.
- (e) data accessed shall be accurate and, every reasonable step must be taken to ensure that personal data which are inaccurate, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

Article 7¹

Data Security

Each Member State shall ensure that data retained under this Framework Decision shall be subject, as a minimum, to the following data security principles and regard shall be given to the provisions of Article 4 of Directive 2002/58/EC :

- (a) the retained data shall be of the same quality 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, alteration, unauthorised disclosure or access, and against all other unlawful forms of processing;
- (c) all data shall be destroyed at the end of the period for retention except those data which have been accessed and preserved;
- (d) the process to be followed in order to get access to retained data and to preserve accessed data shall be defined by each Member State in national law.

¹ Articles 6 and 7 need further consideration.

Article 8

Implementation

Member States shall take the necessary measures to comply with this Framework Decision by [.....June 2007] within two years following the date of adoption.

By the same date Member States shall transmit the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision. The General Secretariat of the Council shall communicate to the Member States the information received pursuant to this Article.

The Commission shall by [....1st January 2008] submit a report to the Council assessing the extent to which the Member States have taken necessary measures in order to comply with this Framework Decision.

Article 9

Entry into force

This Framework Decision shall enter into force on the twentieth day following its publication in the Official Journal of the European Union.
