ARTICLE 29 Data Protection Working Party

654/06/EN
WP 119

Opinion 3/2006
on the Directive 2006/24/EC of the European Parliament and of the Council 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

Adopted on 25 March 2006

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 (1)(a) and (3) of that Directive and 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to its Rules of Procedure, and in particular Articles 12 and 14 thereof,

has adopted the following Opinion:

On 21 February 2006 the Council adopted 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 services and amending Directive 2002/58/EC[2]. The European Parliament had approved the Commission proposal (COM (2005) 0438)[3] as amended during the negotiations with the Council and accordingly adopted a legislative resolution on 14 December 2005 (C6-0293/2005 – 2005/0182(COD)).

In its last Opinion WP 113 of 21 October 2005 on the then draft Directive, the Art. 29 Working Party had voiced its reservations since the provisions of the Directive will have far reaching consequences for all European citizens and their privacy. The decision to retain communication data for the purpose of combating serious crime is an unprecedented one with a historical dimension. It encroaches into the daily life of every citizen and may endanger the fundamental values and freedoms all European citizens enjoy and cherish. The Working Party recalls the considerations and concerns set out in the aforementioned Opinion which retain their validity. It is, therefore, of utmost importance that the Directive is accompanied and implemented in each Member State by measures curtailing the impact on privacy.

The Art. 29 Working Party notes that the Directive lacks some adequate and specific safeguards as to the treatment of communication data and leaves room for diverging interpretation and implementation by the Member States in this respect. However, adequate and specific safeguards are necessary to protect the vital interests of the individual as mentioned by Directive 2002/58/EC, in particular the right to confidentiality when using publicly available electronic communications services. The Working Party considers it also crucial that the provisions of the Directive are interpreted and implemented in a harmonised way to ensure that the European citizens can enjoy throughout the European Union the same level of protection.

Therefore, the Art. 29 Working Party proposes a uniform, European-wide implementation of the Directive. This approach should guarantee a harmonized application of the provisions of the Directive whilst respecting the highest level possible of protecting personal data. This should also be done with a view to reducing the considerable costs to be borne by the service providers when complying with the provisions of the Directive.

In order to transpose the provisions of the Directive in a uniform way and to comply with the requirements of Article 8 of the European Convention on Human Rights, Member States should

1 OJ L 281, 23.11.1995, p. 31, http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm.
2 OJ L 105, 13.04.2006, p.54
3 OJ C 49, 28.2.2006, p. 42.

implement adequate and specific safeguards. At least the following safeguards should be taken into account:

1) **Purpose specification:** The data should only be retained for specific purposes. Therefore, the term "serious crime" should be clearly defined and delineated. Any further processing should be ruled out or limited stringently on the basis of specific safeguards.

2) **Access limitation:** The data should only be available to specifically designated law enforcement authorities where necessary for the investigation, detection, and prosecution of the offences referred to in the Directive. A list of such designated law enforcement authorities should be made public. Any retrieval of the data should be recorded and the records made available to the supervisory authority/ies in order to ensure an effective supervision.

3) **Data minimisation:** The data to be retained should be kept to a minimum, and any changes to that list should be subject to a strict necessity test.

4) **No data mining:** Investigation, detection and prosecution of the offences referred to in the Directive should not entail large-scale data-mining based on retained data, in respect of the travel and communication patterns of people unsuspected by law enforcement authorities.

5) **Judicial/ independent scrutiny of authorized access:** Access to data should, in principle, be duly authorised on a case by case basis by judicial authorities without prejudice to countries where a specific possibility of access is authorised by law, subject to independent oversight. Where appropriate, the authorisations should specify the particular data required for the specific case at hand.

6) **Retention purposes of providers:** Providers of public electronic communication services or networks are not allowed to process data retained solely for public order purposes under the Data Retention Directive for other purposes, especially their own.

7) **System separation:** In particular, the systems for storage of data for public order purposes should be logically separated from the systems used for business purposes.

8) **Security measures:** Minimum standards should be defined concerning the technical and organisational security measures to be taken by providers, specifying more in detail the general requirements of the Directive on data retention.

The Art. 29 Working Party calls on the Member States to co-ordinate the implementation of the data retention Directive into national laws in order to guarantee a harmonised approach across the European Union and to uphold the high standard of data protection provided by both Directives 1995/46/EC and 2002/58/EC.

Done at Brussels, on 25 March 2006

For the Working Party

The Chairman
Peter Schaar