

5085/99/EN/FINAL
WP 25

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

Recommendation 3/99

on

**the preservation of traffic data by Internet Service Providers for law
enforcement purposes**

Adopted on 7 September 1999

Recommendation 3/99
on
the preservation of traffic data by Internet Service Providers for law enforcement purposes

Introduction

Combating computer-related crime is an issue that has been acquiring increasing international attention.¹ The G8 countries² have adopted a 10 point action plan³ which is currently being implemented with the help of a specialised high-tech crime subgroup consisting of representatives G8 law enforcement agencies. One of the outstanding and most controversial issues is the preservation of historic and future traffic data by Internet Service Providers for law enforcement purposes and disclosure of such data to law enforcement authorities. The G8 high-tech crime subgroup intends to propose recommendations to ensure the possibility of preserving and disclosing traffic data. G8 Ministers of Justice and Home Affairs may discuss these recommendations in a meeting in Moscow on 19 – 20 October 1999.

The Working Party on the Protection of Individuals with regard to the Processing of Personal Data⁴ is conscious of the important role that traffic data can play in the context of the investigation of crimes perpetrated over the Internet but wishes however to remind the national governments about the principles on the protection of the fundamental rights and freedoms of natural persons, and in particular of their privacy and the secrecy of their correspondence which need to be taken into account in this context.

The Working Party has understood that the G8 Justice and Home Affairs Ministers may be asked to call for a balanced interpretation of the two EU Data Protection

¹ See for example "COMCRIME Study" "Legal Aspects of computer-related Crime in the Information Society-COMCRIME Study, January 1997 - Delivered within the EU Action Plan against organised crime - Available on the Legal Advisory Board Website : <http://www2.echo.lu/legal/en/comcrime/sieber.html>. The Council of Europe is working on a draft convention on cyber-crime. The EU Council has expressed its support for this work on 27 May 1999. Computer related crime refers to all crimes committed over networks such as computer attacks, publication of illegal material on web sites, including criminal activity committed by transnational organised crime (e.g. narcotics traffickers, child pornographers).

² G8 countries are: Canada, France, Germany, Italy, Japan, the United Kingdom, United States of America and Russia.

³ "Meeting of Justice and Interior Ministers of the Eight December 9-10, 1997, Communiqué, Washington D.C. December 10, Communiqué Annex : Principles and Action Plan to Combat High-tech Crime"

⁴ Instituted by Article 29 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data OJ L 281 of 23.11.1995, p. 31. Available at: <http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm>

Directives⁵ at the stage of implementation that will take into account law enforcement interests alongside privacy interests.

The Working Party is also conscious of the burdens that may be put on telecommunication operators and service providers.

The objective of the present Recommendation is therefore to contribute to an uniform application of Directives 95/46/EC and 97/66/EC with a view to providing for clear and predictable conditions for telecommunications operators and Internet Service Providers as well as for law enforcement authorities whilst preserving the right to privacy.

Legal situation

Within the European Union, Directive 95/46/EC harmonises the conditions of the protection of the right to privacy enshrined in the legal systems of the Member States. This Directive gives substance to and amplifies the principles contained in the European Convention for the Protection of Human Rights of 4 November 1950 and in Council of Europe Convention No. 108 of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. Directive 97/66/EC particularises the provisions of this Directive in the telecommunications sector. Both Directives apply to processing of personal data, including traffic data related to subscribers and users, on the Internet.⁶

In particular Articles 6, 7, 13, 17 (1) and (2) of Directive 95/46/EC and Articles 4, 5, 6 and 14 of Directive 97/66/EC deal with the lawfulness of such processing by telecommunication operators and service providers.

These provisions allow telecommunications operators and telecommunications service providers to process data on telecommunications traffic under certain very limited conditions.

Article 6 (1) lit. b) provides that data may only be collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with the purposes for which the data were collected. Article 6 (1) lit. e) provides that personal data must not be kept longer than is necessary for the purposes for which the data were collected or for which they are further processed. Article 13 allows Member States to restrict the scope of inter alia Article 6 (1) insofar such restriction constitutes a necessary measure to safeguard national security, public security or the prevention, investigation, detection and prosecution of criminal offences.

The application of these principles is further specified in Article 5 and Article 6 paragraphs 2 to 5 of Directive 97/66/EC. Article 5 guarantees the **confidentiality of communications** by means of a public telecommunications network and publicly available telecommunications services. Member States have to prohibit the listening,

⁵ Directive 95/46/EC see footnote 3 and Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, OJ L 24, 30 January 1998, p. 1. Available at: see footnote 4.

⁶ See “Working document: Processing of Personal Data on the Internet”, adopted on 23 February 1999, available at: see footnote 1.

tapping, storage or other kinds of interception or surveillance of communications by others than users, without the consent of the users concerned, except when legally authorised in accordance with Article 14 (1).

As a general rule, **traffic data** must be erased or made anonymous as soon as the communication ends (Article 6 paragraph (1) of Directive 97/66/EC. This is motivated by the sensitivity of traffic data revealing individual communication profiles including information sources and geographical locations of the user of fixed or mobile telephones and the potential risks to privacy resulting from the collection, disclosure or further uses of such data. Exception is made in Article 6 (2) concerning the processing of certain traffic data for the purpose of subscriber billing and interconnection payments, but only up to the end of the period during which the bill may lawfully be challenged or payment may be pursued.

Article 14 (1) allows Member States to restrict the scope of obligations and rights provided for in Article 6 when such restriction constitutes a necessary measure to safeguard national security and the prevention, investigation, detection and prosecutions of criminal offences as referred to in Article 13 (1) of Directive 95/46/EC.

It follows from these provisions, that telecommunications operators and Internet Service providers are not allowed to collect and store data for law enforcement purposes only, unless required to do so by law based on the reasons and under the conditions mentioned above. This is in agreement with longstanding traditions in most Member States, where the application of national data protection principles has resulted in a prohibition for the private sector to keep personal data on the sole basis of potential further need expressed by police or state security forces.

In this context it can be noted that for the purposes of law enforcement and under the conditions contained in Articles 13 of Directive 95/46/EC and Article 14 of Directive 97/66/EC, legislation exists in most Member States defining the precise conditions under which police and state security forces may have *access* to data stored by private telecommunications operators and Internet Service providers for their own civil purposes.

As the Working Party already stated in its Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications adopted on the 3 of May 1999⁷, the fact that a third party acquires knowledge of traffic data concerning the use of telecommunication services has generally been considered as a telecommunication interception and constitutes therefore a violation of the individuals' right to privacy and of the confidentiality of correspondence as guaranteed by Article 5 of directive 97/66/EC⁸. In addition, such disclosure of traffic data is incompatible with Article 6 of that directive.

Any violation of these rights and obligations is unacceptable unless it fulfils three fundamental criteria, in accordance with Article 8 (2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, and the European Court of Human Rights' interpretation of this provision: a legal basis, the need for the measure in a democratic society and conformity with one of the

⁷ Available at: see footnote 1.

⁸ Law enforcement authorities require also access to real-time connection information, data concerning active connections (so-called "future traffic data").

legitimate aims listed in the Convention. The legal basis must precisely define the limits and the means of applying the measure: the purposes for which the data may be processed, the length of time they may be kept (if at all) and access to them must be strictly limited. Large-scale exploratory or general surveillance must be forbidden⁹. It follows that public authorities may be granted access to traffic data only on a case-by-case basis and never proactively and as a general rule.

These criteria coincide with the above mentioned provisions in Article 13 of Directive 95/46/EC and Article 14 of Directive 97/66/EC

Divergence of national rules¹⁰

Concerning the period during which traffic data may be stored, Directive 97/66/EC only allows preservation for billing¹¹ purposes and only up to the end of the period during which the bill may lawfully be challenged. This period however varies significantly in Member States. In Germany for example, telecommunications operators and telecommunications services providers are allowed to store the data necessary for billing up to 80 days for the purpose of proving the correctness of the billing¹². In France, it depends on the status of the operator: the “traditional” telecommunications operator is allowed to keep traffic data up to one year on the basis of the law fixing the period during which the bill can be challenged. This period is fixed to 10 years for other operators. In Austria, the telecommunications law does

⁹ See especially the *Klass* judgment of 6 September 1978, Series A No 28, pp.23 et seq., and the *Malone* judgement of 2 August 1984, Series A No. 82, pp. 30 et seq.

The *Klass* judgement, like the *Leander* judgement of 25 February 1987, insists on the need for “effective guarantees against abuse” “in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it”. (*Leander* judgement, Series A No. 116, pp. 14 et seq.).

The Court notes in the *Klass* judgement (paragraphs 50 et seq.) that assessing the existence of adequate and effective guarantees against abuse depends on all the circumstances of the case. In the particular case, it considers that the surveillance measures provided for in German legislation do not permit exploratory or general surveillance and do not contravene Article 8 of the European Convention for the Protection of Human Rights. German legislation provides the following guarantees: surveillance is confined to cases in which there are indications for suspecting a person of planning, committing or having committed certain serious criminal acts; measures may be ordered only if the establishment of the facts by another method is without prospects of success or considerably more difficult; and even then, the surveillance may cover only the specific suspect or his presumed “contact-persons”.

¹⁰ The Commission is currently in the process of analysing the laws of those Member States who have notified national measures implementing Directive 97/66/EC and Directive 95/46/EC. See implementation table concerning Directive 95/46/EC available at: see footnote 4.

¹¹ And, where necessary, for interconnection payments between telecommunications operators, see Article 6 paragraph 2 of Directive 97/66/EC.

¹² If the bill is challenged during this period, the relevant data can of course be kept until the dispute is settled.

not fix a concrete period up to which traffic data may be stored for billing purposes, but limits it to the period during which the bill can be challenged or during which the payment can be claimed. In the United Kingdom, according to the law, the bill can be challenged during 6 years, but operators and service providers store the relevant data for about 18 month. In Belgium for example, the law does not define such a period, but the biggest telecommunication service provider has fixed this period to 3 month in its general conditions. Another practice can be observed in Portugal where, since the period is not fixed by law, the national data protection supervisory authority decides on a case by case basis. It is interesting to note that in Norway the period is fixed to 14 days.

The current practice of ISPs is also not homogenous: it seems that small ISPs preserve traffic data for very short periods (a few hours) because of lack of storage capacity. Bigger ISPs who are able to afford such storage capacity may be preserving traffic data for up to a few months (but this may depend on their billing policies: per connection time or per fixed period).

For the purpose of law enforcement, the Dutch telecommunications law obliges telecommunications operators and service providers to collect and store traffic data for three month.

Obstacles for the functioning of the Internal Market

This divergence raises potential obstacles within the Internal Market for the cross-border provision of telecommunications and Internet services but as well effective law enforcement may be hampered by such divergent periods. It could be invoked that an ISP established in one Member State is not entitled to store traffic data longer than fixed in the Member State where the customer is living and using its service. Or an ISP may be pressed to keep traffic data longer than allowed in its own Member State because the laws of the country of the users require so. In case of billing for roaming in mobile telephony it is not the foreign operator who recovers the bill, but the national operator of the subscribers concerned. Different periods for storing data necessary for the billing may thus lead to the same problems as described for ISPs.. The rule of the applicable law set out in Article 4 of Directive 95/46/EC does solve this problem only to the extent that the ISP is the controller and established only in one Member State, but not in cases where he is established in several Member States with different periods or where he processes traffic data on behalf of the controller.

Recommendation

In view of the above, the Working Party considers that the most effective means to reduce unacceptable risks to privacy while recognising the needs for effective law enforcement is that traffic data should in principle not be kept only for law enforcement purposes and that national laws should not oblige telecommunications operators, telecommunications service and Internet Service providers to keep traffic data for a period of time longer than necessary for billing purposes.

The Working Party recommends that the European Commission proposes appropriate measures to further harmonise the period for which telecommunication operators, telecommunications service and Internet Service providers are allowed to keep traffic data for billing and interconnection payments¹³. The Working Party considers that this period should be as long as necessary to allow consumers to be able to challenge the billing, but as short as possible in order not to overburden operators and service providers and to respect the proportionality and specificity principles as being part of the right to privacy. This period should be aligned on the highest standard of protection observed in Member States. The group draws attention to the fact, that in several Member States periods of no longer than 3 months have been successfully applied.

The Working Party furthermore recommends that national governments take into account these considerations.

Done at Brussels, 7 September 1999

For the Working Party

The Chairman

Peter HUSTINX

¹³ In view of this objective, there is no justification for operating distinctions relating to private or public operators.