

Electronic communications: personal data protection rules and availability of traffic data for anti-terrorism purposes

2005/0182(COD) - 21/09/2005 - Legislative proposal

PURPOSE : to harmonise provisions concerning processing and retention of data regarding publicly available electronic communications services or public communications for the purpose of preventing and investigating serious criminal offences, and amending Directive 2002/58/EC

PROPOSED ACT : Directive of the European Parliament and of the Council.

CONTENT : Citizens increasingly perform daily activities using electronic communications networks and services. These communications generate 'traffic data' or 'location data' which include details about the location of the caller, the number called, the time and duration of the call. When combined with data

enabling the identification of the user of the service, the availability of such traffic data is important for purposes related to law enforcement. However, with changes in service offerings, such as the growth of flat rate tariffs, pre-paid and free electronic communications services, traffic data may not always be stored by all operators to the same extent as they were in recent years, depending on the services they offer. This trend is reinforced by recent offerings of Voice over IP communication services, or even flat rate services for fixed telephone communications. Under such arrangements, the operators would no longer have the need to store traffic data for billing purposes. If traffic data are not stored for billing or other business purposes, they will not be available for public authorities whenever there is a legitimate case to access the data. These developments are making it much harder for public authorities to fulfil their duties in preventing and combating organised crime and terrorism.

It has now become urgent to adopt harmonised provisions at EU level on this subject. A certain number of Member States have adopted national measures requiring some or all operators to retain given types of data so that they can be used for the purposes identified above when necessary. Differences in the legal, regulatory, and technical provisions in Member States concerning the retention of traffic data present obstacles to the Internal Market for electronic communications as service providers are faced with different requirements regarding the types of data to be retained.

This Directive aims to harmonise the provisions of the Member States concerning obligations on the providers of publicly available electronic communications services or of a public communications network with respect to the processing and retention of certain data, in order to ensure that the data is available for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime. The Directive applies to traffic and location data of both private and legal persons, as well as the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network. The following categories of data must be retained:

- data necessary to trace and identify the source of a communication;
- data necessary to trace and identify the destination of a communication;
- data necessary to identify the date, time and duration of a communication;
- data necessary to identify the type of communication;
- data necessary to identify the communication device;
- data necessary to identify the location of mobile communication equipment.

The types of data to be retained under these categories of data are specified in the Annex.

These categories of data must be retained for a period of one year from the date of the communication, with the exception of data related to electronic communications taking place using wholly or mainly the Internet Protocol. The latter shall be retained for a period of six months.

Statistics on the retention of data must be provided to the European Commission on a yearly basis. Such statistics shall not contain personal data.

Lastly, the Directive must be evaluated three years after transposition.