

Appendix 6

**Directive 2006/24/EC of the European Parliament and of
the Council of 15 March 2006**



Press and Information

Court of Justice of the European Union

PRESS RELEASE No 54/14

Luxembourg, 8 April 2014

Judgment in Joined Cases C-293/12 and C-594/12
Digital Rights Ireland and Seitlinger and Others

The Court of Justice declares the Data Retention Directive to be invalid

It entails a wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary

The main objective of the Data Retention Directive¹ is to harmonise Member States' provisions concerning the retention of certain data which are generated or processed by providers of publicly available electronic communications services or of public communications networks. It therefore seeks to ensure that the data are available for the purpose of the prevention, investigation, detection and prosecution of serious crime, such as, in particular, organised crime and terrorism. Thus, the directive provides that the abovementioned providers must retain traffic and location data as well as related data necessary to identify the subscriber or user. By contrast, it does not permit the retention of the content of the communication or of information consulted.

The High Court (Ireland) and the Verfassungsgerichtshof (Constitutional Court, Austria) are asking the Court of Justice to examine the validity of the directive, in particular in the light of two fundamental rights under the Charter of Fundamental Rights of the EU, namely the fundamental right to respect for private life and the fundamental right to the protection of personal data.

The High Court must resolve a dispute between the Irish company Digital Rights Ireland and the Irish authorities regarding the legality of national measures concerning the retention of data relating to electronic communications. The Verfassungsgerichtshof has before it several constitutional actions brought by the Kärntner Landesregierung (Government of the Province of Carinthia) and by Mr Seitlinger, Mr Tschohl and 11 128 other applicants. Those actions seek the annulment of the national provision which transposes the directive into Austrian law.

By today's judgment, the Court declares the directive invalid².

The Court observes first of all that the data to be retained make it possible, in particular, (1) to know the identity of the person with whom a subscriber or registered user has communicated and by what means, (2) to identify the time of the communication as well as the place from which that communication took place and (3) to know the frequency of the communications of the subscriber or registered user with certain persons during a given period. Those data, taken as a whole, may provide very precise information on the private lives of the persons whose data are retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, activities carried out, social relationships and the social environments frequented.

The Court takes the view that, **by requiring the retention of those data and by allowing the competent national authorities to access those data, the directive interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data.** Furthermore, the fact that data are retained and subsequently used without the

¹ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 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 (OJ 2006 L 105, p. 54).

² Given that the Court has not limited the temporal effect of its judgment, the declaration of invalidity takes effect from the date on which the directive entered into force.

subscriber or registered user being informed is likely to generate in the persons concerned a feeling that their private lives are the subject of constant surveillance.

The Court then examines whether such an interference with the fundamental rights at issue is justified.

It states that **the retention of data** required by the directive **is not such as to adversely affect the essence of the fundamental rights to respect for private life and to the protection of personal data**. The directive does not permit the acquisition of knowledge of the content of the electronic communications as such and provides that service or network providers must respect certain principles of data protection and data security.

Furthermore, the retention of data for the purpose of their possible transmission to the competent national authorities **genuinely satisfies an objective of general interest, namely the fight against serious crime and, ultimately, public security**.

However, the Court is of the opinion that, by adopting the Data Retention Directive, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality.

In that context, the Court observes that, in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right caused by the directive, the EU legislature's discretion is reduced, with the result that review of that discretion should be strict.

Although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, **the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary**.

Firstly, the directive covers, in a generalised manner, all individuals, all means of electronic communication and all traffic data without **any differentiation, limitation or exception** being made in the light of the objective of fighting against serious crime.

Secondly, the directive fails to lay down any objective criterion which would ensure that the competent national authorities have **access to the data** and can use them only for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights in question, may be considered to be sufficiently serious to justify such an interference. On the contrary, the directive simply refers in a general manner to 'serious crime' as defined by each Member State in its national law. In addition, the directive does not lay down substantive and procedural conditions under which the competent national authorities may have access to the data and subsequently use them. In particular, the access to the data is not made dependent on the prior review by a court or by an independent administrative body.

Thirdly, so far as concerns **the data retention period**, the directive imposes a period of at least six months, without making any distinction between the categories of data on the basis of the persons concerned or the possible usefulness of the data in relation to the objective pursued. Furthermore, that period is set at between a minimum of six months and a maximum of 24 months, but the directive does not state the objective criteria on the basis of which the period of retention must be determined in order to ensure that it is limited to what is strictly necessary.

The Court also finds that the directive does not provide for sufficient safeguards to ensure effective protection of the data against the **risk of abuse** and against any unlawful access and use of the data. It notes, inter alia, that the directive permits service providers to have regard to economic considerations when determining the level of security which they apply (particularly as regards the costs of implementing security measures) and that it does not ensure the irreversible destruction of the data at the end of their retention period.

Lastly, the Court states that the directive does **not** require that the data be **retained within the EU**. Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.

NOTE: A reference for a preliminary ruling allows the courts and tribunals of the Member States, in disputes which have been brought before them, to refer questions to the Court of Justice about the interpretation of European Union law or the validity of a European Union act. The Court of Justice does not decide the dispute itself. It is for the national court or tribunal to dispose of the case in accordance with the Court's decision, which is similarly binding on other national courts or tribunals before which a similar issue is raised.

Unofficial document for media use, not binding on the Court of Justice.

The [full text](#) of the judgment is published on the CURIA website on the day of delivery.

Press contact: Christopher Fretwell ☎ (+352) 4303 3355

Pictures of the delivery of the judgment are available from "[Europe by Satellite](#)" ☎ (+32) 2 2964106

**DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 15 March 2006**

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission,

Having regard to the Opinion of the European Economic and Social Committee ⁽¹⁾,

Acting in accordance with the procedure laid down in Article 251 of the Treaty ⁽²⁾,

Whereas:

- (1) 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 ⁽³⁾ requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.
- (2) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ⁽⁴⁾ translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.
- (3) Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be

erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value-added services.

- (4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.
- (5) Several Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of criminal offences. Those national provisions vary considerably.
- (6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.
- (7) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth in the possibilities afforded by electronic communications, data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of criminal offences, in particular organised crime.
- (8) 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.

⁽¹⁾ Opinion delivered on 19 January 2006 (not yet published in the Official Journal).

⁽²⁾ Opinion of the European Parliament of 14 December 2005 (not yet published in the Official Journal) and Council Decision of 21 February 2006.

⁽³⁾ OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

⁽⁴⁾ OJ L 201, 31.7.2002, p. 37.

- (9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, *inter alia*, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.
- (10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.
- (11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.
- (12) Article 15(1) of Directive 2002/58/EC continues to apply to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this Directive and which therefore fall outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive.
- (13) This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data should be retained in such a way as to avoid their being retained more than once. Data generated or processed when supplying the communications services concerned refers to data which are accessible. In particular, as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers' or the network providers' own services.
- (14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve. In order to obtain advice and encourage the sharing of experience of best practice in these matters, the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament and data protection authorities, including the European Data Protection Supervisor.
- (15) Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive. Article 30(1)(c) of Directive 95/46/EC requires the consultation of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of that Directive.
- (16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.
- (17) It is essential that Member States adopt legislative measures to ensure that data retained under this Directive are provided to the competent national authorities only in accordance with national legislation in full respect of the fundamental rights of the persons concerned.
- (18) In this context, Article 24 of Directive 95/46/EC imposes an obligation on Member States to lay down sanctions for infringements of the provisions adopted pursuant to that Directive. Article 15(2) of Directive 2002/58/EC imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58/EC. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems ⁽¹⁾ provides that the intentional illegal access to information systems, including to data retained therein, is to be made punishable as a criminal offence.
- (19) 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 that Directive, applies also in relation to the unlawful processing of any personal data pursuant to this Directive.

⁽¹⁾ OJ L 69, 16.3.2005, p. 67.

- (20) The 2001 Council of Europe Convention on Cybercrime and 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 this Directive.
- (21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.
- (22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.
- (23) Given that the obligations on providers of electronic communications services should be proportionate, this Directive requires that they retain only such data as are generated or processed in the process of supplying their communications services. To the extent that such data are not generated or processed by those providers, there is no obligation to retain them. This Directive is not intended to harmonise the technology for retaining data, the choice of which is a matter to be resolved at national level.
- (24) In accordance with paragraph 34 of the Interinstitutional agreement on better law-making ⁽¹⁾, Member States are encouraged to draw up, for themselves and in the interests of the Community, their own tables illustrating, as far as possible, the correlation between this Directive and the transposition measures, and to make them public.
- (25) This Directive is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. Issues of access to data retained pursuant to this Directive by national authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community

law. However, they may be subject to national law or action pursuant to Title VI of the Treaty on European Union. Such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as guaranteed by the ECHR. Under Article 8 of the ECHR, as interpreted by the European Court of Human Rights, interference by public authorities with privacy rights must meet the requirements of necessity and proportionality and must therefore serve specified, explicit and legitimate purposes and be exercised in a manner that is adequate, relevant and not excessive in relation to the purpose of the interference,

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter and scope

1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.
2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to 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.

Article 2

Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) ⁽²⁾, and in Directive 2002/58/EC shall apply.
2. For the purpose of this Directive:
 - (a) 'data' means traffic data and location data and the related data necessary to identify the subscriber or user;

⁽¹⁾ OJ C 321, 31.12.2003, p. 1.

⁽²⁾ OJ L 108, 24.4.2002, p. 33.

- (b) 'user' means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;
- (c) 'telephone service' means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);
- (d) 'user ID' means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;
- (e) 'cell ID' means the identity of the cell from which a mobile telephony call originated or in which it terminated;
- (f) 'unsuccessful call attempt' means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

Article 3

Obligation to retain data

1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.

2. The obligation to retain data provided for in paragraph 1 shall include the retention of the data specified in Article 5 relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by providers of publicly available electronic communications services or of a public communications network within the jurisdiction of the Member State concerned in the process of supplying the communication services concerned. This Directive shall not require data relating to unconnected calls to be retained.

Article 4

Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance

with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

- (a) data necessary to trace and identify the source of a communication:
- (1) concerning fixed network telephony and mobile telephony:
 - (i) the calling telephone number;
 - (ii) the name and address of the subscriber or registered user;
 - (2) concerning Internet access, Internet e-mail and Internet telephony:
 - (i) the user ID(s) allocated;
 - (ii) the user ID and telephone number allocated to any communication entering the public telephone network;
 - (iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;
- (b) data necessary to identify the destination of a communication:
- (1) concerning fixed network telephony and mobile telephony:
 - (i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;
 - (ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

- (2) concerning Internet e-mail and Internet telephony:
- (i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;
 - (ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;
- (c) data necessary to identify the date, time and duration of a communication:
- (1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;
 - (2) concerning Internet access, Internet e-mail and Internet telephony:
 - (i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;
 - (ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;
- (d) data necessary to identify the type of communication:
- (1) concerning fixed network telephony and mobile telephony: the telephone service used;
 - (2) concerning Internet e-mail and Internet telephony: the Internet service used;
- (e) data necessary to identify users' communication equipment or what purports to be their equipment:
- (1) concerning fixed network telephony, the calling and called telephone numbers;
 - (2) concerning mobile telephony:
 - (i) the calling and called telephone numbers;
 - (ii) the International Mobile Subscriber Identity (IMSI) of the calling party;
 - (iii) the International Mobile Equipment Identity (IMEI) of the calling party;
- (iv) the IMSI of the called party;
- (v) the IMEI of the called party;
- (vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;
- (3) concerning Internet access, Internet e-mail and Internet telephony:
- (i) the calling telephone number for dial-up access;
 - (ii) the digital subscriber line (DSL) or other end point of the originator of the communication;
- (f) data necessary to identify the location of mobile communication equipment:
- (1) the location label (Cell ID) at the start of the communication;
 - (2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.
2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Article 7

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 this Directive:

- (a) the retained data shall be of the same quality and 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, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
- (c) the data shall be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;
- and
- (d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

Member States shall ensure that the data specified in Article 5 are retained in accordance with this Directive in such a way that the data retained and any other necessary information relating to such data can be transmitted upon request to the competent authorities without undue delay.

Article 9

Supervisory authority

- Each Member State shall designate one or more public authorities to be responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to Article 7 regarding the security of the stored data. Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC.
- The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

Article 10

Statistics

1. Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network. Such statistics shall include:

- the cases in which information was provided to the competent authorities in accordance with applicable national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,

— the cases where requests for data could not be met.

- Such statistics shall not contain personal data.

Article 11

Amendment of Directive 2002/58/EC

The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:

'1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (*) to be retained for the purposes referred to in Article 1(1) of that Directive.

(*) OJ L 105, 13.4.2006, p. 54.'

Article 12

Future measures

- A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them.
- The Commission shall, within a period of six months after the notification referred to in paragraph 1, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within that period the national measures shall be deemed to have been approved.
- Where, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may consider whether to propose an amendment to this Directive.

Article 13

Remedies, liability and penalties

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 any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.

Article 14

Evaluation

1. No later than 15 September 2010, the Commission shall submit to the European Parliament and the Council an evaluation of the application of this Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission pursuant to Article 10 with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data in Article 5 and the periods of retention provided for in Article 6. The results of the evaluation shall be made public.

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party established under Article 29 of Directive 95/46/EC.

Article 15

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than 15 September 2007. They shall forthwith inform the Commission thereof. When Member States adopt those measures, they shall contain a reference to this Directive or

shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

3. Until 15 March 2009, each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the *Official Journal of the European Union*.

Article 16

Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Article 17

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 15 March 2006.

For the European Parliament
The President
J. BORRELL FONTELLES

For the Council
The President
H. WINKLER

Declaration by the Netherlands
pursuant to Article 15(3) of Directive 2006/24/EC

Regarding the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC, the Netherlands will be making use of the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period not exceeding 18 months following the date of entry into force of the Directive.

Declaration by Austria
pursuant to Article 15(3) of Directive 2006/24/EC

Austria declares that it will be postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail, for a period of 18 months following the date specified in Article 15(1).

Declaration by Estonia
pursuant to Article 15(3) of Directive 2006/24/EC

In accordance with Article 15(3) of the Directive 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, Estonia hereby states its intention to make use of use that paragraph and to postpone application of the Directive to retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption of the Directive.

Declaration by the United Kingdom
pursuant to Article 15(3) of Directive 2006/24/EC

The United Kingdom declares in accordance with Article 15(3) of the Directive 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 that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Cyprus
pursuant to Article 15(3) of Directive 2006/24/EC

The Republic of Cyprus declares that it is postponing application of the Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until the date fixed in Article 15(3).

Declaration by the Hellenic Republic
pursuant to Article 15(3) of Directive 2006/24/EC

Greece declares that, pursuant to Article 15(3), it will postpone application of this Directive in respect of the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 18 months after expiry of the period provided for in Article 15(1).

Declaration by the Grand Duchy of Luxembourg
pursuant to Article 15(3) of Directive 2006/24/EC

Pursuant to Article 15(3) of the Directive 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, the Government of the Grand Duchy of Luxembourg declares that it intends to make use of Article 15(3) of the Directive in order to have the option of postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Slovenia**pursuant to Article 15(3) of Directive 2006/24/EC**

Slovenia is joining the group of Member States which have made a declaration under Article 15(3) of the Directive of the European Parliament and 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, for the 18 months postponement of the application of the Directive to the retention of communication data relating to Internet, Internet telephony and Internet e-mail.

Declaration by Sweden**pursuant to Article 15(3) of Directive 2006/24/EC**

Pursuant to Article 15(3), Sweden wishes to have the option of postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Lithuania**pursuant to Article 15(3) of Directive 2006/24/EC**

Pursuant to Article 15(3) of the draft Directive 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 public communications networks and amending Directive 2002/58/EC (hereafter the 'Directive'), the Republic of Lithuania declares that once the Directive has been adopted it will postpone the application thereof to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for the period provided for in Article 15(3).

Declaration by the Republic of Latvia**pursuant to Article 15(3) of Directive 2006/24/EC**

Latvia states in accordance with Article 15(3) of Directive 2006/24/EC of 15 March 2006 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 that it is postponing application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 15 March 2009.

Declaration by the Czech Republic**pursuant to Article 15(3) of Directive 2006/24/EC**

Pursuant to Article 15(3), the Czech Republic hereby declares that it is postponing application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail until 36 months after the date of adoption thereof.

Declaration by Belgium**pursuant to Article 15(3) of Directive 2006/24/EC**

Belgium declares that, taking up the option available under Article 15(3), it will postpone application of this Directive, for a period of 36 months after its adoption, to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by the Republic of Poland**pursuant to Article 15(3) of Directive 2006/24/EC**

Poland hereby declares that it intends to make use of the option provided for under Article 15(3) of the Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of publicly available electronic communications services and amending Directive 2002/58/EC and postpone application of the Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in Article 15(1).

Declaration by Finland**pursuant to Article 15(3) of Directive 2006/24/EC**

Finland declares in accordance with Article 15(3) of the Directive 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 that it will postpone application of that Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail.

Declaration by Germany**pursuant to Article 15(3) of Directive 2006/24/EC**

Germany reserves the right to postpone application of this Directive to the retention of communications data relating to Internet access, Internet telephony and Internet e-mail for a period of 18 months following the date specified in the first sentence of Article 15(1).
