EUROPEAN PARLIAMENT

2004 *2009*

Committee on Civil Liberties, Justice and Home Affairs

27.10.2005 PE 364.849v01-00

AMENDMENTS 44-238

Draft report **(PE 364.679v01-00)**
Alexander Nuno Alvaro
on the proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC

Proposal for a directive (COM(2005)0438 – C6-0293/2005 – 2005/0182(COD) – amending act)

Text proposed by the Commission	Amendments by Parliament

Amendment by Jean-Marie Cavada

Amendment 44
Recital 3

(3) Articles ***5,*** 6 and 9 of Directive 2002/58/EC define 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***	(3) Articles 6 and 9 of Directive 2002/58/EC define the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. ***In principle such*** data *should* be erased or made anonymous when no longer needed for the purpose of the transmission of a communication: ***For the purposes of subscriber*** billing ***and*** interconnection payments ***data may be processed, but only up to end of the period during which the***

purposes and the provision of value added services.	***bill may lawfully be challenged of payment may be pursued;***

Or. en

Amendment by Charlotte Cederschiöld

Amendment 45
Recital 4

(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 the Directive; any such derogations need to 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.***	(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 the Directive; any such derogations need to 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 investigation, detection and prosecution of ***serious*** criminal offences.

Or. en

Justification

As hacking and other attacks on electronic communications systems are included in serious criminal offences there is no need for this clarification. However, when downloading and file sharing of i.e. music becomes a criminal offence under the pending IPR enforcement directive it should not fall under the scope of this directive as this directive is meant to protect citizens against terrorism and serious crime.

Amendment by Jean-Marie Cavada

Amendment 46
Recital 4

(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	(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 inter alia***

Article 5, Article 6***, Article 8(1)(2)(3) and (4),*** and Article 9 of the Directive; any such derogations need to 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.	Article 6 and Article 9 of the Directive; any such derogations need to 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;

Or. en

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler and Stavros Lambrinidis

Amendment 47
Recital 4 a (new)

	4a Article 7 of the Charter of Fundamental Rights explicitly recognises the right to respect for private life and Article 8 thereof the right to protection of personal data.

Or. fr

Amendment by Sylvia-Yvonne Kaufmann

Amendment 48
Recital 5

(5) ***Several*** Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of crime and criminal offences; the provisions of the various national legislations vary considerably.	(5) ***Ten of the 25*** Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of crime and criminal offences***, which in some cases has not yet been implemented;*** the provisions of the various national legislations vary considerably.

Or. de

Justification

The amendment specifies the number of Member States that have adopted some kind of legislation on data retention.

Amendment by Jean-Marie Cavada

Amendment 49
Recital 5

(5) ***Several*** Member States have adopted ***legislation*** providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of crime and criminal offences; ***the provisions of the various national legislations vary considerably.***	(5) ***Some*** Member States have adopted ***national legislations*** providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of crime and criminal offences;

Or. en

Amendment by Edith Mastenbroek, Lilli Gruber and Stavros Lambrinidis

Amendment 50
Recital 5

(5) ***Several*** Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of crime and criminal offences; the provisions of the various national legislations vary considerably.	(5) ***Some*** Member States have adopted legislation providing for the retention of data by service providers for the prevention, investigation, detection, and prosecution of crime and criminal offences;; the provisions of the various national legislations vary considerably.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 51
Recital 5

(5) ***Several*** Member States have adopted legislation providing for the retention of data by service providers for the ***prevention,*** investigation, detection, and prosecution of crime and criminal offences; the provisions of the various national legislations vary considerably.	(5) ***Only a few*** Member States have adopted legislation providing for the retention of data by service providers for the investigation, detection, and prosecution of crime and criminal offences; the provisions of the various national legislations vary considerably.

Or. en

Amendment by Ioannis Varvitsiotis

Amendment 52
Recital 5

(5) Several Member States have adopted legislation providing for the retention of data by service providers for the ***prevention,*** investigation, detection, and prosecution of crime and criminal offences; the provisions of the various national legislations vary considerably.	(5) Several Member States have adopted legislation providing for the retention of data by service providers for the investigation, detection, and prosecution of crime and criminal offences; the provisions of the various national legislations vary considerably.

Or. en

Amendment by Jean-Marie Cavada

Amendment 53
Recital 6

(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; service providers are faced with different*** requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention.	(6) The ***provisions so far adopted present*** legal and technical differences ***and the*** requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention ***also differ.***

Or. en

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 54
Recital 6

(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of prevention, investigation, detection and	(6) 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; service providers are faced with different requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention.	prosecution of criminal offences ***may become*** obstacles to the internal market for electronic communications; service providers are faced with different requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 55
Recital 6

(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; service providers are faced with different requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention.	(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of investigation, detection and prosecution of ***serious*** criminal offences present obstacles to the internal market for electronic communications; service providers are faced with different requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention.

Or. en

Justification

The purpose of this Directive is said to be to combat serious criminal offences, such as terrorism and organised crime. The word serious should then be used in every case.

Amendment by Ioannis Varvitsiotis

Amendment 56
Recital 6

(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	(6) The legal and technical differences between national provisions concerning the retention of data for the purpose of investigation, detection and prosecution of criminal offences present obstacles to the internal market for electronic

electronic communications; service providers are faced with different requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention.

communications; service providers are faced with different requirements regarding the types of traffic data to be retained as well as the conditions and the periods of retention.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 57
Recital 6 a (new)

(6) a The harmonisation of the internal market in the field of data retention highlights the need for a better and more equal access to justice and appeal for citizens, throughout the EU. Every citizen should have the same right to legal protection and compensation against misuse of information regardless if it originates from an authority or a provider.

Or. en

Amendment by Edith Mastenbroek, Lilli Gruber and Stavros Lambrinidis

Amendment 58
Recital 7

(7) The Conclusions of the Justice and Home Affairs Council of 20 September 2001 call for ensuring that law enforcement authorities are able to investigate criminal acts which involve the use of electronic communications and to take legal measures against perpetrators of these crimes, while striking a balance between the protection of personal data and the needs of law enforcement authorities to gain access to data for criminal investigation purposes.

(7) The Conclusions of the Justice and Home Affairs Council of 20 September 2001 call for ensuring that law enforcement authorities are able to investigate criminal acts which involve the use of electronic communications and to take legal measures against perpetrators of these crimes, while striking a balance between ***respect for fundamental rights and*** the protection of personal data***,*** and the needs of law enforcement authorities to gain access to data for criminal investigation purposes.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 59
Recital 7

(7) The Conclusions of the Justice and Home Affairs Council of 20 September 2001 call for ensuring that law enforcement authorities are able to investigate criminal acts which involve the use of electronic communications and to take legal measures against perpetrators of these crimes, while striking a balance between the protection of personal data and the needs of law enforcement authorities to gain access to data for criminal investigation purposes.	(7) The Conclusions of the Justice and Home Affairs Council of 20 September 2001 call for ensuring that law enforcement authorities are able to investigate ***serious*** criminal acts which involve the use of electronic communications and to take legal measures against perpetrators of these crimes, while striking a balance between the protection of personal data and the needs of law enforcement authorities to gain access to data for criminal investigation purposes.

Or. en

Justification

The word "serious" should apply to criminal acts throughout the text.

Amendment by Charlotte Cederschiöld

Amendment 60
Recital 8

(8) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications is particularly important and therefore a valuable tool in the prevention, investigation, detection and prosecution of crime and criminal offences, in particular against organised crime.	***deleted***

Or. en

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 61
Recital 8

(8) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications ***is particularly important and therefore*** a valuable tool in the prevention, investigation, detection and prosecution of crime and criminal offences, in particular against organised crime.	(8) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications ***may be*** a valuable tool in the prevention, investigation, detection and prosecution of crime and criminal offences, in particular against organised crime.

Or. en

Amendment by Ioannis Varvitsiotis

Amendment 62
Recital 8

(8) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications is particularly important and therefore a valuable tool in the ***prevention,*** investigation, detection and prosecution of crime and criminal offences, in particular against organised crime.	(8) The Conclusions of the Justice and Home Affairs Council of 19 December 2002 underline that, because of the significant growth of the possibilities of electronic communications, data relating to the use of electronic communications is particularly important and therefore a valuable tool in the investigation, detection and prosecution of crime and criminal offences, in particular against organised crime.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 63
Recital 9

(9) The Declaration on combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for	***deleted***

establishing rules on the retention of communications traffic data by service providers.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 64
Recital 10

(10) The declaration adopted by the special informal Council of 13 July 2005 reinforces the need to adopt measures related to the retention of electronic communications traffic data as soon as possible.	***deleted***

Or. en

Amendment by Jean-Marie Cavada

Amendment 65
Recital 10

(10) The declaration adopted by the special informal Council of 13 July 2005 reinforces the need to adopt measures related to the retention of electronic communications traffic data as soon as possible.	(10) The declaration adopted by the special informal Council of 13 July 2005 reinforces the need to adopt ***common*** measures related to the retention of electronic communications traffic data as soon as possible.

Or. en

Amendment by Jean-Marie Cavada

Amendment 67
Recital 10 a (new)

	(10a) The Working Party on the protection of individuals with regard to processing of personal data established according to

Article 29 of Directive 95/46/EC shall carry out the tasks laid down in Article 30 of the abovementioned Directive also with regard to the protection of fundamental rights and freedoms and of legitimate interests in the sector which is subject to this Directive.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 68
Recital 11

(11) ***Given the importance of traffic data for the prevention, investigation, detection, and prosecution of serious criminal offences, such as terrorism and organised crime, as demonstrated by research and the practical experience of several Member States, there is a need to ensure that data which are*** processed by electronic communication providers when offering public electronic communication services or public communication networks are retained for a ***certain*** period of time.	(11) ***Data*** processed by ***public*** electronic communication providers when offering public electronic communication services or public communication networks are ***to be*** retained for a ***harmonised*** period of time.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 69
Recital 11

(11) Given the importance of traffic data for the ***prevention,*** investigation, detection, and prosecution of serious criminal offences, such as terrorism and organised crime, as demonstrated by ***research and*** the practical experience of several Member States, there is a need to ensure that data which are processed by electronic communication providers when offering ***public*** electronic communication services or ***public*** communication networks are retained for a ***certain*** period of time.	(11) Given the ***potential*** importance of traffic data for the prevention, investigation, detection, and prosecution of serious criminal offences, such as terrorism and organised crime, as demonstrated by the practical experience of several Member States, there is a need to ensure that data which are processed by electronic communication providers when offering ***publicly accessible*** electronic communication services or ***publicly accessible*** communication networks are

retained for a ***standard*** period of time.

Or. de

Justification

Parliament has not been presented with any scientific studies dealing with the comprehensive retention of traffic data. Traffic data are usually just one of many pieces of evidence that play a part in the investigation of serious criminal offences.

Amendment by Ioannis Varvitsiotis

Amendment 70
Recital 11

(11) Given the importance of traffic data for the ***prevention,*** investigation, detection, and prosecution of serious criminal offences, ***such as terrorism and organised crime,*** as demonstrated by research and the practical experience of several Member States, there is a need to ensure that data which are processed by electronic communication providers when offering public electronic communication services or public communication networks are retained for a certain period of time.	(11) Given the importance of traffic data for the investigation, detection, and prosecution of serious criminal offences, ***as those are defined by each Member State, and*** as demonstrated by research and the practical experience of several Member States, there is a need to ensure that data which are processed by electronic communication providers when offering public electronic communication services or public communication networks are retained for a certain period of time.

Or. en

Justification

It is not necessary at this stage to give examples of what is a serious criminal offence. Each Member State has the right to define the case of a serious criminal offence.

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 71
Recital 11

(11) Given the importance of traffic data for the prevention, investigation, detection, and prosecution of serious criminal offences, such as terrorism and organised crime, as demonstrated by research and the practical experience of several Member States, there	Given the importance of traffic data for the prevention, investigation, detection, and prosecution of serious criminal offences, such as terrorism and organised crime, as demonstrated by research and the practical experience of several Member States, there

is a need to ensure that data which are processed by electronic communication providers when offering public electronic communication services or public communication networks are retained for a certain period of time.	***may be*** a need to ensure that data which are processed by electronic communication providers when offering public electronic communication services or public communication networks are retained for a certain period of time.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 72
Recital 11 a (new)

(11a) The drawing up of any lists of types of data to be retained should reflect a balance between the benefit to the investigation, detection and prosecution of serious criminal offences against the degree of invasion of privacy which will result. Any crime on such a list should meet up to the proportionality demand and pass a necessity test as stipulated in the Treaty.

Or. en

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 73
Recital 11 a (new)

(11a) For the purpose of this Directive electronic communications and electronic communications traffic data mean: fixed network and mobile telephony.

Or. en

Justification

The necessity of mandatory retention of internet traffic data has not been proven. Storing internet traffic data is much more difficult than phone data, internet traffic data is far less reliable than phone data, and internet traffic data is far less useful than phone data. Internet data retention is easy to avoid by abusing innocent people. On top of this, the open and decentralized character of the internet is threatened by data retention. And other, more

targeted measures are available and waiting to be implemented.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 74
Recital 12

(12) ***The categories of information to be retained reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause; the applicable retention period of one year, respectively six months where data relate to electronic communications taking place using solely the Internet Protocol, also strikes a reasonable balance between all the interests involved.***	(12) ***A general retention period of three months reflects a sensible approach to harmonisation, in the light of current practice in the European Union and given that the period can be extended if necessary, if there is sufficient suspicion.***

Or. de

Justification

As comprehensive data retention substantially impinges on EU citizens' fundamental rights, the harmonised retention period should be kept short in order to minimise this impingement.

Amendment by Charlotte Cederschiöld

Amendment 75
Recital 12

(12) The categories of information to be retained reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause; the applicable retention period ***of one year, respectively six months where data relate to electronic communications taking place using solely the Internet Protocol, also strikes a reasonable balance between all the interests involved.***	***(12) Due to the uncertainty of the efficiency of this method*** the applicable retention period ***should be harmonised three months as a clear majority of all requests on data retained refers to data not older than the above stated period.***

Or. en

Amendment by Jean-Marie Cavada

Amendment 76
Recital 12

(12) The categories of information to be retained reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause***; the applicable retention period of one year, respectively six months where data relate to electronic communications taking place using solely the Internet Protocol, also strikes a reasonable balance between all the interests involved.***	(12) The categories of information to be retained ***and the retention period of one year, respectively six months where data relate to electronic communications taking place using solely the Internet Protocol,*** reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause***.***

Or. en

Amendment by Ioannis Varvitsiotis

Amendment 77
Recital 12

(12) The categories of information to be retained reflect an appropriate balance between the benefits for the ***prevention,*** investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause; the applicable retention period of ***one year***, respectively ***six months*** where data relate to electronic communications taking place using solely the Internet Protocol, also strikes a reasonable balance between all the interests involved.	(12) The categories of information to be retained reflect an appropriate balance between the benefits for the investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause; the applicable retention period of ***six months***, respectively ***three months*** where data relate to electronic communications taking place using solely the Internet Protocol, also strikes a reasonable balance between all the interests involved.

Or. en

Justification

In view of the cost and the use of the data, we support a shorter period of data retention.

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 78
Recital 12

(12) The categories of information to be retained reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause; the applicable retention period ***of one year, respectively six months where data relate to electronic communications taking place using solely the Internet Protocol,*** also strikes ***a reasonable*** balance between all the interests involved.	(12) The categories of information to be retained ***should*** reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause; the applicable retention period ***should*** also strike ***an appropriate*** balance between all the interests involved.

Or. en

Amendment by Herbert Reul

Amendment 79
Recital 12

(12) ***The categories of information to be retained reflect an appropriate balance between the benefits for the prevention, investigation, detection, and prosecution of the serious offences involved and the level of invasion of privacy they will cause;*** the applicable retention period of ***one year, respectively six months where data relate to electronic communications taking place using solely the Internet Protocol,*** also strikes a reasonable balance between all the interests involved.	(12) the applicable retention period of ***six months*** also strikes a reasonable balance between all the interests involved.

Or. de

Justification

Experience in the Member States shows that a retention period of six months already suffices for the authorities' greatest needs. In the light of this, and out of particular concern for the fundamental rights of those citizens affected, a six-month retention period for all data types

seems to be sufficient and proportionate.

Amendment by Stavros Lambrinidis, Edith Mastenbroek

Amendment 80
Recital 12 a (new)

(12a) Whereas in the Paper by the UK Presidency of the Council entitled "Liberty and Security: Striking the Right Balance," the Presidency notes that, "in the future some criminals and terrorists will adapt their use of technology to make the retention of this data a less important tool for investigations," thus underlying the need for the thorough future review of the necessity, proportionality, and effectiveness of the present Directive, as well as the need for the collection of appropriate statistical data on the implementation of this Directive, in order to facilitate such a review.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 81
Recital 13

(13) Given the fact that retention of data generates significant additional costs for electronic communication providers***, whilst the benefits in terms of public security impact on society in general,*** it is appropriate to foresee that Member States reimburse demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.	(13) Given the fact that retention of data generates significant additional costs for ***public*** electronic communication providers, ***which can not be avoided to be paid by consumers of telecom services*** it is appropriate to foresee that Member States reimburse demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.

Or. en

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 82
Recital 13

(13) Given the fact that retention of data generates significant additional costs for electronic communication providers, whilst the benefits in terms of public security impact on society in general, it is appropriate to foresee that Member States reimburse demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.	(13) Given the fact that retention of data generates significant additional costs for electronic communication providers, whilst the ***expected*** benefits in terms of public security impact on society in general, it is appropriate to foresee that Member States reimburse demonstrated additional costs incurred in order to comply with the obligations imposed on them as a consequence of this Directive.

Or. en

Amendment by Jean-Marie Cavada

Amendment 83
Recital 14

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission envisages ***to create a*** platform composed of representatives of the law enforcement authorities, associations of the electronic communications industry and data protection authorities.	(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission envisages ***a periodic review of the strict necessity of such provisions and the evaluation of the types of data that are needed. A*** platform composed of representatives of the ***European Parliament,*** law enforcement authorities, associations of the electronic communications industry and ***European and national*** data protection authorities ***may assist the Commission.***

Or. en

Amendment by Charlotte Cederschiöld

Amendment 84
Recital 14

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission envisages to create a platform composed of representatives of the law enforcement authorities, ***associations of*** the electronic communications industry and data protection authorities.	(14) Technologies relating to electronic communications are changing rapidly and ***would*** the legitimate requirements of the competent authorities ***as well as those of the providers*** evolve; ***no decision should be taken within the comitology procedure or within*** a platform ***but should include the European Parliament,*** law enforcement authorities, the electronic communications industry and ***European and national*** data protection authorities.

Or. en

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 85
Recital 14

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission ***envisages to*** create a platform composed of representatives of the law enforcement authorities, associations of the electronic communications industry and data protection authorities.	(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve; to advise on these matters the Commission ***will*** create a ***consultative*** platform composed of representatives of the law enforcement authorities, associations of the electronic communications industry***, civil rights and user organisations, the European Parliament*** and data protection authorities***, including the European Data Protection Supervisor***.

Or. en

Amendment by Jean-Marie Cavada

Amendment 86
Recital 15

(15) It should be recalled that 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 'Article 29 Working Party'.***	(15) It should be recalled that Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive, ***in particular mention should be made of Article 15(2) and (3) of Directive 95/46/EC.***

Or. en

Amendment by Stavros Lambrinidis, Edith Mastenbroek

Amendment 87
Recital 16

(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.	(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms. ***Such measures should necessarily include strict technical requirements and obligations on the part of both, providers and authorities to safeguard the data from unauthorized or other inappropriate or unlawful storage, access, processing, disclosure, sharing, or use, as well as effective and enforceable penal sanctions with a sufficient deterrent effect in the event of the intentional or negligent failure of providers, relevant authorities, or their employees to fully safeguard such data.***

Or. en

Justification

The protection of the fundamental rights of citizens in the present case must necessarily involve protection of the retained data from any unauthorized or unlawful access, use, or other interference, both from the outside (e.g., hackers, trojan horses, etc.) and from the inside (abuse by companies storing the data or by the authorities accessing them, and their employees). Furthermore, unless the integrity of the data can be guaranteed, their evidentiary value in any investigation would be open to challenge. Strict penal sanctions on providers and Authorities who fail to ensure, whether intentionally or negligently, the integrity and confidentiality of the data is a necessary component of assuring citizens that their fundamental rights in this instance will be protected.

Amendment by Charlotte Cederschiöld

Amendment 88
Recital 16

(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.	(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions ***such as the requirement of suspicion in relation of a specific serious criminal offence***, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.

Or. en

Amendment by Ioannis Varvitsiotis

Amendment 89
Recital 16

(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.	(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation ***and within the provisions of the national judicial system, and following the approval of the judicial authorities,*** in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and

Fundamental freedoms.

Or. en

Justification

There must be a control when the data are provided.

Amendment by Jean-Marie Cavada

Amendment 90
Recital 16

(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.	(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms ***and in the Charter of Fundamental Rights of the European Union.*** ***To this end it is necessary for Member States to ensure that the national data protection authorities can be approached by any person who suspects that personal data is being used for purposes other than those set out in this directive. The European Parliament urges Member States to equip those national authorities with means of control that are in step with the development of communications.***

Or. fr

Justification

National data protection commissions have been set up in all Member States to protect and ensure respect for the private lives of European citizens, and it is their responsibility to make

sure that this is indeed the case.

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 91
Recital 16

(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.	(16) It is essential that Member States provide legislative measures to ensure that data retained under this Directive are only provided to the competent national authorities in accordance with national legislation in full respect of the fundamental rights of the persons concerned, ***while respecting data protection principles***; such measures include in particular appropriate conditions, limits and safeguards in order to ensure the conformity of the provision of the data retained with fundamental rights as guaranteed in particular in the European Convention for the Protection of Human Rights and Fundamental freedoms.

Or. en

Amendment by Jean-Marie Cavada, Edith Mastenbroek, Lilli Gruber and Charlotte Cederschiöld

Amendment 92 to 94
Recital 17

(17) The measures necessary for the implementation of this Directive should be adopted in accordance with Council Decision 1999/468/EC of 28 June 1999 laying down the procedures for the exercise of implementing powers conferred on the Commission[1].	***deleted***

Or. en

Amendment by Charlotte Cederschiöld

[1] OJ L 184, 17.7.1999, p. 23.

Amendment 95
Recital 18

(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the ***prevention,*** investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore 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.	(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore 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, ***it is unclear whether*** this Directive does not go beyond what is necessary ***and proportionate*** in order to achieve those objectives, ***as also pointed out by the European Data Protection Supervisor.***

Or. en

Amendment by Ioannis Varvitsiotis

Amendment 96
Recital 18

(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the ***prevention,*** investigation, detection and prosecution of serious criminal offences***, such as terrorism and organised crime,*** cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore 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	(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the investigation, detection and prosecution of serious criminal offences cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore 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

Directive does not go beyond what is necessary in order to achieve those objectives.	necessary in order to achieve those objectives.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 97
Recital 18

(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the ***prevention***, investigation, detection and prosecution of serious criminal offences, ***such as terrorism and organised crime***, cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore 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.	(18) The objectives of the action to be taken, namely to harmonise the obligations on providers to retain certain data and to ensure that these data are available for the purpose of the investigation, detection and prosecution of ***certain*** serious criminal offences, cannot be sufficiently achieved by the Member States and can, by reason of the scale and effects of the action, be better achieved at Community level. Therefore 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.

Or. de

Justification

Consequential amendment.

Amendment by Charlotte Cederschiöld

Amendment 98
Recital 19

(19) 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	(19) This Directive ***could better*** *respect* the fundamental rights and the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union; in particular, this Directive together with

together with Directive 2002/58/EC, seeks to ensure full respect of the fundamental rights to respect the private life and communications of citizens and the protection of personal data (Articles 7 and 8 of the Charter),	Directive 2002/58/EC, ***and*** seek to ensure full respect of the fundamental rights to respect the private life and communications of citizens and the protection of personal data (Articles 7 and 8 of the Charter) ***as well as the judgments of the European Court of Human Rights[1].***
	[1] See in particular the judgments in the cases Amann v. Switzerland (no. 27798/95, ECHR 2000-II of 16 February 2000, where the storing of information about an individual was considered to be an interference with private life, even though it contained no sensitive data) and Malone v the United Kingdom (no. 8691/79, of 2 August 1984, where the same applied to the practice of 'metering' of telephone calls, which involves the use of a device that registers automatically the numbers dialled on a telephone and the time and duration of each call).

Or. en

Amendment by Charlotte Cederschiöld

Amendment 99
Article 1, paragraph 1

1. 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.	1. 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, ***and to ensure proportionality and necessity and that the rights to respect for private life and to the protection of personal data in the access of these data are fully respected,*** in order to ensure that the data is available for the purpose of the investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime ***referred to in paragraph 2a.***

Or. en

Justification

Excluding prevention and location data limits the possibility of mapping and profiling 457 million European citizens.

Amendment by Jean-Marie Cavada

Amendment 100
Article 1, paragraph 1

1. 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.	1. 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, ***access and use of the retained data,*** in order to ensure that the data is available for the purpose of the investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.

Or. en

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 101
Article 1, paragraph 1

1. 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.	1. This Directive aims to harmonise the provisions of ***the laws of some*** 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.

Or. en

Amendment by Bill Newton Dunn

Amendment 102
Article 1, paragraph 1

1. 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.***	1. 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 criminal offences**.**

Or. en

Justification

Data retention requirements are of primary importance to allow law enforcement measures and judicial proceedings to be taken against all forms of online crimes. Without a requirement to retain data, authorities face significant obstacles in tracking illegal activities and identifying suspected infringers, and in talking actions to enforce offences and legal rights. This Directive should therefore cover all forms of criminal offences.

Amendment by Ioannis Varvitsiotis

Amendment 103
Article 1, paragraph 1

1. 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***.	1. 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 investigation, detection and prosecution of serious criminal offences.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 104
Article 1, paragraph 1

1. 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***.	1. 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 ***publicly accessible electronic*** 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 investigation, detection and prosecution of ***the*** criminal offences ***referred to in paragraph 2a.***

Or. de

Justification

The wording 'serious criminal offences, such as terrorism and organised crime' can be broadly interpreted by the individual Member States. This will lead to difficulties when data comes to be exchanged in line with the principle of availability and a criminal offence is not classed as a serious criminal offence in both Member States. A list of serous criminal offences would therefore be preferable.

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler and Stavros Lambrinidis

Amendment 105
Article 1, paragraph 1

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.	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 ***and access to and the use of data retained***, 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 ***and that it is adequately protected***.

Or. fr

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 106
Article 1, paragraph 2

2. This Directive shall apply 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.***	2. This Directive shall apply 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 communications.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 107
Article 1, paragraph 2

2. This Directive shall apply 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.	2. This Directive shall apply to traffic 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.

Or. en

Justification

Excluding prevention and location data limits the possibility of mapping and profiling 457 million European citizens.

Amendment by Jean-Marie Cavada

Amendment 108
Article 1, paragraph 2

2. This Directive shall apply 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.***	2. This Directive shall apply 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.

Or. en

Amendment by Sarah Ludford

Amendment 109
Article 1, paragraph 2

2. This Directive shall apply 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.	This Directive shall apply to ***records of*** 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. ***It shall not apply to data which is processed only as required for transmission through the network where no non-transient record is made.***

Or. en

Justification

It is not possible to store all the communications data that passes through a network. The appropriate place to make such records is at the network edge.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 110
Article 1, paragraph 2

2. This Directive shall apply 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.	2. This Directive shall apply to ***traffic data*** of both private and legal persons, as well as ***those*** 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.

Or. de

Justification

The deletion of 'location data' should prevent a complete record of citizens' movements being formed and retained. 'Related' is too broad a term. Only the data directly and absolutely necessary for the identification of the subscriber or user should be retained.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 111
Article 1, paragraph 2 a (new)

	2a. The following shall be criminal offences within the meaning of paragraph 1:
	- membership of a criminal organisation,
	- terrorism,
	- arms trafficking
	- trafficking in persons,
	- sexual exploitation of children and child pornography,
	- illegal trading in drugs and psychotropic substances,
	- laundering of the proceeds of crime,
	- counterfeiting, including counterfeiting of the euro,
	- environmental crime, including illegal trading in threatened animal or plant and tree species,
	- homicide, grievous bodily harm,
	- illegal trading in organs and human tissue,
	- kidnapping, holding persons against their will and hostage-taking,
	- forging of official documents and trading

in such forged documents,
- forging of means of payment,
- illegal trading in nuclear and radioactive substances,
- rape,
- arson,
- crimes which fall within the jurisdiction of the International Criminal Court,
- hijacking of aircraft and ships,

Or. de

Justification

The wording 'serious criminal offences, such as terrorism and organised crime' can be broadly interpreted by the individual Member States. This will lead to difficulties when data comes to be exchanged in line with the principle of availability and a criminal offence is not classed as a serious criminal offence in both Member States. A list of serous criminal offences would therefore be preferable.

Amendment by Jean-Marie Cavada

Amendment 112
Article 1, paragraph 2 a (new)

2a. The Directive shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Or. en

Amendment by Sarah Ludford

Amendment 113
Article 2, paragraph 2 a (new)

2a. "Internet communications" means all communications transmitted through a public electronic communications network using the Internet protocol other than those whose destination is primarily identified to the relevant electronic communications network provider by a telephone number

that is part of a National Numbering Plan

Or. en

Justification

The words "to the electronic communications network provider" are crucial to resolve the problem of calls between the Internet and the telephone networks, which are Internet communications while on the Internet but telephony while on the telephone networks.

Amendment by Jean-Marie Cavada

Amendment 114
Article 2, paragraph 2, point a)

a) 'data' means traffic data and location data, as well as the related data necessary to identify the subscriber or user;	***deleted***

Or. en

Amendment by Sarah Ludford

Amendment 115
Article 2, paragraph 2, point a)

a) 'data' means traffic data and location data, as well as the related data necessary to identify the subscriber or user;	a) 'data' means ***records that have been made of*** traffic data and location data, as well as the related data necessary to identify the subscriber or user;

Or. en

Justification

To ensure consistency with the amendment on Article 1.2

Amendment by Charlotte Cederschiöld

Amendment 116
Article 2, paragraph 2, point a)

a) ‘data’ means traffic data ***and location data***, as well as the ***related*** data necessary to identify the subscriber or user;	a) ‘data’ means traffic data, as well as the data necessary to identify the subscriber or user;

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 117
Article 2, paragraph 2(a)

(a) ‘data’ means traffic data and ***location data, as well as the related*** data necessary to identify the subscriber or user;	(a) ‘data’ means traffic data and ***those*** data necessary to identify the subscriber or user;

Or. de

Justification

The deletion of 'location data' should prevent a complete record of citizens' movements being formed and retained. 'Related' is too broad a term. Only the data directly and absolutely necessary for the identification of the subscriber or user should be retained.

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 118
Article 2, paragraph 2

2. For the purpose of this Directive:	2. For the purpose of this Directive:
	a) ‘electronic communications and electronic communications traffic data’ means fixed network and mobile telephony;
a) ‘data’ means traffic data ***and location data,*** as well as the related data necessary to identify the subscriber or user;	*b)* ‘data’ means traffic data, as well as the related data necessary to identify the subscriber or user;
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 this***	*c)* ‘user’ means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes.

service.

Or. en

Amendment by Jean-Marie Cavada

Amendment 119
Article 2, paragraph 2, point ba) (new)

ba) 'serious criminal offences' means the offences referred to in Article 2(2) of the Council Framework Decision 2002/584/JHA[1].

[1] Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 120
Article 2, paragraph 2, point ba) (new)

ba) 'competent law enforcement authorities' means the National Board of Police in each Member State.

Or. en

Justification

It is important to control number of institutions with access to the data retained in order to limit the risks for citizens. The definition of the authorities in "other authorities responsible for the detection, investigation and prosecution of serious criminal offences" is neither clear nor harmonised. As exchange of retained data is foreseen the number of individuals with access to the data will be undefined and numerous in a union of 25 Member States.

Amendment by Jean-Marie Cavada

Amendment 121
Article 2, paragraph 2, point bb) new

bb) 'unsuccessful call attempt' means a communication in which a telephone call has been successfully connected but is unanswered or there has been a network management intervention.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 122
Article 2, paragraph 2 (ba) (new)

(ba) 'competent authorities' means judicial authorities and authorities responsible for the detection, investigation and punishment of serious criminal offences. Secret services are not 'competent authorities'.

Or. de

Justification

Clarification and restriction of access to data.

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler, Stavros Lambrinidis

Amendment 123
Article 2, paragraph 2, point (b a) (new)

ba) 'competent national authorities' means the judicial authorities and national authorities responsible for the investigation, detection and prosecution of serious criminal offences.

Or. fr

Amendment by Herbert Reul

Amendment 124
Article 3, paragraph 1

1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which 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 communication services ***are retained*** in accordance with the provisions of this Directive.	1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that***, in the event of a successfully established connection, providers of publicly available electronic communications services or of a public communications network providing the service in question retain and make available*** data which are generated or processed in the process of supplying communication services in accordance with the provisions of this Directive. ***This shall not affect the right of Member States to apply their national constitutional and other legal principles with regard to confidentiality in communication areas particularly protected under basic rights such as communication by and with journalists and defence lawyers and members of other professions required to uphold confidentiality.***

Or. de

Justification

Only the company providing the service in question should be obliged to retain data, as this company alone has control of the relevant data. Unsuccessful call attempts should not be subject to the obligation to retain data, as this would result in high investment costs disproportionate to the expected investigative value for the law enforcement authorities.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 125
Article 3, paragraph 1

1. ***By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC,*** Member States shall adopt measures to ensure that data which are ***generated or*** processed by providers of publicly available electronic communications services or of a ***public***	1. Member States shall adopt measures to ensure that data which are processed ***during a communication*** by providers of publicly available electronic communications services or of a ***publicly accessible electronic*** communications network within

communications network within their jurisdiction in the process of supplying communication services are retained in accordance with the provisions of this Directive.	their jurisdiction in the process of supplying communication services are retained in accordance with the provisions of this Directive.

Or. de

Justification

The deletion restricts the amount of data to be retained and makes clear that unsuccessful call attempts are not to be included.

Amendment by Jean-Marie Cavada

Amendment 126
Article 3, paragraph 1

1. By way of derogation to Articles ***5,*** 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that ***data which 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 communication services ***are retained*** in accordance with the provisions of this Directive.	1. By way of derogation to Articles 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that providers of publicly available electronic communications services or of a public communications network within their jurisdiction ***retain data which they control for the purpose*** of supplying ***their*** communication services in accordance with the provisions of this Directive. ***This Directive does not require providers of electronic communications services or networks to generate or process additional data beyond that required for the provision of their services, nor to verify the accuracy of the data not generated by them.***

Or. en

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler and Stavros Lambrinidis

Amendment 127
Article 3, paragraph 1

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

Or. fr

Amendment by Sarah Ludford

Amendment 128
Article 3, paragraph 1

1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which 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 communication services are retained in accordance with the provisions of this Directive.	1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that ***records that are generated of*** data which 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 communication services are retained in accordance with the provisions of this Directive.

Or. en

Justification

Consequent to amendment on Article 1.2.

Amendment by Charlotte Cederschiöld

Amendment 129
Article 3, paragraph 1

1. ***By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC,*** Member States shall adopt measures to ensure that data which are generated or processed by providers of publicly available electronic communications services or of a public	1. Member States shall adopt measures to ensure that data which 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

communications network within their jurisdiction in the process of supplying communication services are retained in accordance with the provisions of this Directive.	communication services are retained in accordance with the provisions of this Directive, ***for a specific serious criminal offence.***

Or. en

Justification

Derogating from Articles 5, 6 and 9 in Directive 2002/58/EC is regulated in Article 15 (1) of the same Directive. Derogations are allowed for "criminal offences" and "for unauthorised use of the electronic communications systems".

When the pending Intellectual Property Rights (IPR) Enforcement Directive COM (2005)276 is adopted, unauthorised downloading and file sharing will become a criminal offence and thus fall under the scope of this Directive.

If this is the intention of the Directive, it should be clearly stated to the legislator and the public.

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 130
Article 3, paragraph 1

1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which 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 communication services are retained in accordance with the provisions of this Directive.	1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which are ***processed and logged*** by providers of publicly available communications services or of a public communications network within their jurisdiction in the process of supplying communication services are retained in accordance with the provisions of this Directive.

Or. en

Amendment by Wolfgang Kreissl-Dörfler

Amendment 131
Article 3, paragraph 1

1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which 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 communication services are retained in accordance with the provisions of this Directive.	1. By way of derogation to Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that data which are generated or processed ***in the event of a successfully established connection or during a communication*** by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying communication services are retained in accordance with the provisions of this Directive.

Or. de

Justification

The retention of unsuccessful call attempts should be explicitly ruled out. There has been no evidence so far of law enforcement authorities needing urgently to resort to this kind of data. It is far more likely that a huge amount of data would have to be collected, the retention of which would result in enormous investment costs. A measure of this kind exceeds the realms of proportionality.

Amendment by Kathalijne Maria Buitenweg

Amendment 132
Article 3, paragraph 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime**.**	2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities ***through a push system***, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime ***and only when the person whose data are requested is reasonably suspected of having committed or of planning to commit a criminal offence.***

Or. en

Amendment by Sarah Ludford

Amendment 133
Article 3, paragraph 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.	2. Member States shall adopt measures to ensure that data ***related to the services provided and*** retained in accordance with this Directive are only provided to the competent national authorities ***by the provider offering the e-communication service to the end user***, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.

Or. en

Justification

To ensure legal certainty, this article needs to be further clarified in order to identify the service providers falling under the scope of the proposed Directive, in other words which are the service providers obliged to retain and provide what data for LEAs purposes?

Any obligation to retain specific data referring relating to the destination of a communication (e.g. name and address of the subscriber or registered recipient, connection label or user ID of the intended recipients, IMSI, IMEI of the called party) is virtually impossible whenever it involves different service providers, as it is often the case within a liberalized environment with multiple actors in the marketplace.

Only the party offering the respective service can be subject to the data retention obligation. This party is the only one to have a direct relationship with the customer and with sovereignty over the data ("data controller" based on the definition of the Framework Data Protection Directive, Dir. 95/46/EC).

As an example, those companies which act only as mere carriers can't identify the final subscriber of an email service, only the service provider with a direct relationship with the end user is able to provide this information.

Amendment by Jean-Marie Cavada

Amendment 134
Article 3, paragraph 2

2. Member States shall adopt measures to	2. Member States shall adopt measures to

ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with ***national legislation,*** for the purpose of the prevention, investigation, detection and prosecution of ***serious criminal offences, such as*** terrorism and organised crime.	ensure that data retained in accordance with this Directive are only provided to the competent national authorities and in specific cases in accordance ***with the provisions of this Directive*** for the purpose of the prevention, investigation, detection and prosecution of terrorism and organised crime.

Or. en

Amendment by Ioannis Varvitsiotis

Amendment 135
Article 3, paragraph 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the ***prevention,*** investigation, detection and prosecution of serious criminal offences***, such as terrorism and organised crime***.	2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, ***following the approval of the judicial authorities,*** in specific cases and in accordance with national legislation ***and within the provisions of the national judicial system***, for the purpose of the investigation, detection and prosecution of serious criminal offences.

Or. en

Justification

We have to ensure that individuals other than the competent authorities do not have access to that data.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 136
Article 3, paragraph 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the ***prevention***, investigation, detection and	2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of

prosecution of ***serious*** criminal offences***, such as terrorism and organised crime***.	***the*** criminal offences ***referred to in Article 1(2a)***.

Or. de

Justification

The wording 'serious criminal offences, such as terrorism and organised crime' can be broadly interpreted by the individual Member States. This will lead to difficulties when data comes to be exchanged in line with the principle of availability and a criminal offence is not classed as a serious criminal offence in both Member States. A list of serous criminal offences would therefore be preferable. The use of traffic data for the prevention of criminal offences is conceivable only by means of filtering all the data available. However, the searching of all data without grounds for suspicion is a severe infringement of basic rights and cannot be permitted.

Amendment by Bill Newton Dunn

Amendment 137
Article 3, paragraph 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are ***only*** provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of ***serious*** criminal offences***, such as terrorism and organised crime.***	2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided to the competent national authorities, in specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of criminal offences***.***

Or. en

Justification

Data retention requirements are of primary importance to allow law enforcement measures and judicial proceedings to be taken against all forms of online crimes. Without a requirement to retain data, authorities face significant obstacles in tracking illegal activities and identifying suspected infringers, and in talking actions to enforce offences and legal rights. This Directive should therefore cover all forms of criminal offences.

Amendment by Charlotte Cederschiöld

Amendment 138
Article 3, paragraph 2

2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national ***authorities***, in specific cases and in accordance with national legislation, for the purpose of the ***prevention,*** investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.	2. Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national ***authority***, in specific cases and in accordance with national legislation, for the purpose of the investigation, detection and prosecution of serious criminal offences, ***referred to in Article 1, paragraph 2a.*** ***This Directive shall comply with the principles laid down in the Council Framework Decision on [data protection].***

Or. en

Justification

As long as the scope of this Directive is not entirely clear and transparent no further Directives laying down detailed rules should be initialized.

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler and Stavros Lambrinidis

Amendment 139
Article 3, paragraph 2

Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national ***authorities, in*** specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.	Member States shall adopt measures to ensure that data retained in accordance with this Directive are only provided to the competent national ***authorities in*** specific cases and in accordance with national legislation, for the purpose of the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime.

Or. fr

Amendment by Jean-Marie Cavada

Amendment 140
Article 3, paragraph 2 a (new)

	2a. To this end an updated list of the designated competent law enforcements authorities should be publicly available.

Or. en

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler, Giovanni Claudio Fava

Amendment 141
Article 3 a (new)

Article 3a

Access to retained data

Member States shall adopt measures to ensure that the competent law enforcement authorities are granted access to data retained following the decision of a judicial authority and in accordance with this Directive, only subject to the following conditions:

a) access is granted when necessary, proportionate and appropriate for specified, explicit and legitimate purposes on a case by case basis and in accordance with national law for the prevention, investigation, detection and prosecution of serious criminal offences;

b) the data requested is necessary, proportionate and appropriate to the purpose and in the context of a specific investigation, and does not include large scale data-mining or other similar requests;

c) the competent law enforcement authorities do not process further or use the data in a way, which is incompatible with the purposes for which it was requested; any further use or processing by them for other related proceedings or purposes or any access by other government bodies to the same data requires the filing of a new access application;

d) the process to be followed in order to get access to retained data and to preserve accessed data is defined by each Member State in national law; providers of publicly available electronic communications services or networks guarantee effectively that access is only granted to the competent law enforcement authorities; providers are

strictly prohibited from accessing, processing, using, sharing, or otherwise utilizing data retained under this Directive for purposes other than those explicitly stated in this Directive or in Directive 2002/58/EC regarding their normal business purposes;

e) any accessing of retained data is recorded in a data processing register that enables identification of the requester, the data controllers, the personnel authorised to access and process the data, the judicial authorisation in question, the data consulted and the purpose for which they have been consulted;

f) the competent law enforcement authorities keep the data in a form which allows data subjects to be identified only for as long as is necessary for the purpose for which the data were collected or processed further;

g) the competent law enforcement authorities safeguard the confidentiality and integrity of the data;

h) the competent law enforcement authorities forward the data to third countries, or other third party only under special circumstances.

Or. xm

Amendment by Sylvia-Yvonne Kaufmann

Amendment 142
Article 3 a (new)

Article 3a

Access to data

The Member States shall ensure that the competent authorities have access, in line with national legislation, to the data retained under this Directive, provided that:

a) access is for the purpose of the investigation, detection and prosecution of

the criminal offences under Article 1(2a) and this is confirmed by a court order,

b) the competent authorities keep the data retained and transmitted to them pursuant to this Directive only as long as is required for the investigation, detection and prosecution of criminal offences under Article 1(2a),

c) the competent authorities take appropriate measures to guarantee the confidentiality of the data in their possession retained pursuant to this Directive,

d) the competent authorities do not transmit any data to third countries.

Or. de

Justification

The European Data Protection Supervisor has recommended that rules on access and data protection should be included in this directive in order to prevent the misuse of retained data.

Amendment by Jean-Marie Cavada

Amendment 143
Article 3 a (new)

Article 3a

Access to retained data

1. Each Member State shall ensure that access to data retained under this Directive is subject, as a minimum, to the following conditions and shall establish judicial remedies in line with the provisions of Chapter III of Directive 95/46/EC:

(a) data is accessed for specified, explicit and legitimate purposes by competent law enforcement authorities duly authorised and on a case by case basis in accordance with national law;
(b) the competent law enforcement authorities do not process further the data in a way, which is incompatible with those purposes; any further processing of

retained data by competent law enforcement authorities for other related proceedings should be limited on the basis of stringent safeguards;
(c) any access to the data by other government bodies is prevented;
(d) access to retained data by any other third parties is illegitimate;
(e) the process to be followed in order to get access to retained data and to preserve accessed data is defined by each Member State in their national law; providers are not allowed to process data retained under this Directive for their own purposes;
(f) the data are adequate, relevant and are not excessive in relation to the purposes for which they were accessed. Data are processed fairly and lawfully: in any case access is restricted to those data that are necessary in the context of a specific investigation and does not include large-scale data-mining in respect of travel and communications patterns of people unsuspected by the competent law enforcement authorities;
(g) the competent law enforcement authorities keep the data in a form which allows data subjects to be identified only for as long as is necessary for the purpose for which the data were collected or processed further;
(h) the competent law enforcement authorities safeguard the confidentiality and integrity of the data; they record any retrieval of the data and make these records available to the national data protection authorities;
(i) data accessed are accurate and, every necessary step is 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.

Or. en

Amendment by Stavros Lambrinidis, Edith Mastenbroek

Amendment 144
Article 3 a (new)

Article 3a

Member States shall adopt measures to ensure that the competent law enforcement authorities are granted access to data retained following the decision of a judicial authority and in accordance with this Directive, only subject to the following conditions:

(a) access is granted when necessary, proportionate and appropriate for specified, explicit and legitimate purposes on a case by case basis and in accordance with national law for the prevention, investigation, detection and prosecution of serious criminal offences;
(b) the data requested are necessary, proportionate and appropriate to the purpose and in the context of a specific investigation, and does not include large scale data-mining or other similar requests; request for data, especially when for the purpose of preventing a serious crime, shall be based strictly on concrete evidence;
(c) the competent law enforcement authorities do not process further or use the data in a way, which is incompatible with the purposes for which it was requested; any further use or processing by them for other proceedings or purposes or any access by other government bodies to the same data requires the filing of a new access application;
(d) the process to be followed in order to get access to retained data and to preserve accessed data is defined by each Member State in their national law; providers guarantee effectively that access is only granted to the competent authorities; providers are strictly prohibited from accessing, processing, using, sharing, or otherwise utilizing data retained under this

Directive for purposes other than those explicitly stated in this Directive or in Directive 2002/58/EC regarding their normal business purposes;
(e) every access to retained data is registered to a special register that allows the identification of
(i) the employee or employees accessing, processing and/or transferring the data,
(ii) the requesting authority,
(iii) the relevant judicial authorization,
(iv) the accessed data, and
(v) the purpose for which the data is being accessed;
(f) the competent law enforcement authorities keep the data in a form which allows data subjects to be identified only for as long as is necessary for the purpose for which the data were collected or processed further;
(g) the competent law enforcement authorities safeguard the confidentiality and integrity of the data;
the competent law enforcement authorities do not forward the data to third countries, or any other third party.

Or. en

Justification

European law, including Article 15 of Directive 2002/58/EC, requires that access to data be necessary, proportionate, and appropriate within a democratic society before it is granted. Furthermore, for purposes of the evaluation of the application of the Directive by the Institutions, it is important that all data regarding individual cases be retained in a special register.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 145
Article 3 b (new)

Article 3b

Legal Protection Supervisor

1. After consulting its national Data Protection Supervisor and the Presidents of its national Constitutional Court and national Administrative Court, each Member State shall appoint a Legal Protection Supervisor, who shall be responsible for checking the legality of measures taken pursuant to this Directive, and two deputy supervisors to two-year terms of office. Those terms of office may be renewed.

2. The Legal Protection Supervisor and his/her deputy supervisors must have exceptional knowledge of and experience in the areas of fundamental rights and freedoms and law enforcement. They must have adequate professional experience in a profession requiring a degree in law. Member States shall ensure that persons currently working for an authority as defined in Article 1(2c) are not appointed as Legal Protection Supervisors.

3. The Legal Protection Supervisor shall carry out his/her duties independently and shall not be bound by instructions. He/she shall be required to comply with the rules on official secrecy. His/her deputies shall have the same rights and obligations. Member States shall take appropriate measures to ensure that the Legal Protection Supervisor is provided with the staff he/she needs to perform his/her administrative duties and to meet his/her practical requirements.

4. The Legal Protection Supervisor shall be responsible for the legal scrutiny of all measures taken by authorities and other persons in connection with this Directive. In that connection, he/she shall have the right to inspect all necessary documents and to be provided with all necessary information. However, this right shall not cover information whose disclosure would endanger national security or the security of individuals. Official secrecy may not be invoked as grounds for denying him/her

information.

5. The Legal Protection Supervisor shall submit an annual report to the Commission on measures taken under this Directive. The Commission shall make such reports available to the European Parliament and the Council at their request.

6. Should the Legal Protection Supervisor establish that an individual's rights have been violated as a result of the use of data without that individual's knowledge, he/she shall be empowered:

(1) to notify the individual concerned; or

(2) to lodge a complaint with the competent data protection supervisor. A complaint pursuant to point (2) shall be admissible only if disclosure of the substance of the data set to the individual concerned would compromise or seriously hamper the investigation or prosecution of criminal offences and notification cannot therefore be given pursuant to point (1).

Or. de

Justification

The concept of the Legal Protection Supervisor is taken from Austrian law. Under that country's legal system, this post has been established, alongside the Data Protection Commission, in all areas where the authorities deal with sensitive personal data. The establishment of this post has reduced the number of requests from the authorities for access to such data.

Amendment by Jean-Marie Cavada

Amendment 146
Article 3 b (new)

Article 3b

Data Protection and Data security

Providers of publicly available electronic communications services or networks shall ensure that the systems for storage of data for public order purposes should be logically separated from system that are

used for their business purposes.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 147
Article 3 c (new)

Article 3c

Data protection and data security

1. Each Member State shall ensure that at least the security standards laid down in Article 17 of Directive 95/46/EC apply to the data retained pursuant to this Directive and that the arrangements for the exchange of such data are consistent with the provisions of Article 4 of Directive 2000/58/EC.

2. Under no circumstances may such data be passed on to third countries.

3. Operators of publicly available electronic communication services shall undertake to comply with the security standards laid down in paragraph 1.

4. Under no circumstances may such data be used for commercial purposes. Operators of publicly available electronic communication services shall voluntarily give a corresponding undertaking.

Or. de

Justification

With a view to preventing any misuse of retained data, the European Data Protection Supervisor has recommended that provisions governing access to and protection of data should be incorporated into this directive.

Amendment by Michael Cashman

Amendment 148
Article 4, title

Categories of data to be retained	Categories ***and types*** of data to be retained

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 149
Article 4, title

Categories of data to be retained	Categories ***and types*** of data to be retained

Or. de

Justification

Follow-up amendment.

Amendment by Kathalijne Maria Buitenweg

Amendment 150
Article 4

Member States shall ensure that the following categories of data are retained under this Directive:	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; (b) data necessary to trace and identify the destination of a communication; (c) data necessary to identify the date, time and duration of a communication; (d) data necessary to identify the type of communication; (e) data necessary to identify the communication device or what purports to be the communication device; (f) data necessary to identify the location of mobile communication equipment. The types of data to be retained under the abovementioned categories of data are specified ***in the Annex.***	(a) data necessary to trace and identify the source of a communication; (b) data necessary to trace and identify the destination of a communication; (c) data necessary to identify the date, time and duration of a communication; (d) data necessary to identify the type of communication; (e) data necessary to identify the communication device or what purports to be the communication device; (f) data necessary to identify the location of mobile communication equipment. The types of data to be retained under the abovementioned categories of data are specified ***as follows:***
	a) Data necessary to trace and identify the source of a communication:
	(1) Concerning Fixed Network

Telephony:

(a) The calling telephone number;

(b) Name and address of the subscriber or registered user;

(2) Concerning Mobile Telephony:

(a) The calling telephone number;
(b) Name and Address of the subscriber or registered user;

b) Data necessary to trace and identify the destination of a communication:

(1) Concerning Fixed Network Telephony:

(a) The called telephone number or numbers;

(2) Concerning Mobile Telephony:

(a) The called telephone number or numbers;

c) Data necessary to identify the date, time and duration of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony:

(a) The date and time of the start and end of the communication.

d) Data necessary to identify the type of communication:

(1) Concerning Fixed Network Telephony:

(a) The telephone service used, e.g. voice, conference call, fax and messaging services.

(2) Concerning Mobile Telephony:

(a) The telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service.

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

(1) Concerning Mobile Telephony:

(a) The International Mobile Subscriber Identity (IMSI) of the calling and called party;

(b) The International Mobile Equipment Identity (IMEI) of the calling and called party.

f) Data necessary to identify the location of mobile communication equipment:

(1) The location label (Cell ID) at the start and end of the communication;

(2) Data mapping between Cell IDs and their geographical location at the start and end of the communication.

Or. en

(....)

Justification

Inclusion in article 4 of the parts of the annex relating to telephone communications and excluding any reference to internet data

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 151
Article 4

Categories of data to be retained	Categories ***and types*** **of** data to be retained
Member States shall ensure that ***the following categories of data are retained under this Directive:***	***1.*** Member States shall ensure that ***only those categories and types of data are retained which are processed and logged by providers of publicly available communications services or of a public communications network.***
	2.This Directive refers to the following categories of data:
(a) data necessary to trace and identify the source of a communication; (b) data necessary to trace and identify the destination of a communication; (c) data necessary to identify the date, time and duration of a communication;	(a) data necessary to trace and identify the source of a communication; (b) data necessary to trace and identify the destination of a communication; (c) data necessary to identify the date, time and duration of a communication;

(d) data necessary to identify the type of communication;
(e) data necessary to identify the communication device or what purports to be the communication device;
(f) data necessary to identify the location of mobile communication equipment.
The types of data to be retained under the abovementioned categories of data are specified in the Annex.

(d) data necessary to identify the type of communication;
(e) data necessary to identify the communication device or what purports to be the communication device;
(f) data necessary to identify the location of mobile communication equipment.
3. This Directive refers to the following types of data:

a) Data necessary to trace and identify the source of a communication:
(1) Concerning Fixed Network Telephony:
(a) The calling telephone number;
(b) Name and address of the subscriber or registered user;
(2) Concerning Mobile Telephony:
(a) The calling telephone number;
(b) Name and Address of the subscriber or registered user;
b) Data necessary to trace and identify the destination of a communication:
(1) Concerning Fixed Network Telephony:
(a) The called telephone number or numbers;
(b) Name(s) and Address(es) of the subscriber(s) or registered user(s);
(2) Concerning Mobile Telephony:
(a) The called telephone number or numbers;
(b) Name(s) and Address(es) of the subscriber(s) or registered user(s);
c) Data necessary to identify the date, time and duration of a communication:
(1) Concerning Fixed Network Telephony and Mobile Telephony:
(a) The date and time of the start and end of the communication
d) Data necessary to identify the type of communication:

(1) Concerning Fixed Network Telephony:

(a) The telephone service used, e.g. voice, conference call, fax and messaging services.

(2) Concerning Mobile Telephony:

(a) The telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service.

e) Data necessary to identify the location of mobile communication equipment:

(1) The location label (Cell ID) at the start and end of the communication;

(2) Data mapping between Cell IDs and their geographical location at the start and end of the communication.

Data that reveals the content of a communication may not be included.

Or. en

(....)

Justification

The proposal for retention of phone and internet traffic data appears to be based on the idea that telecom and internet networks are comparable. This is not the case. The internet should not be included in the directive. Reasons are the lack of balance between risks and benefits, and the negative impact on innovation.

The necessity of mandatory retention of internet traffic data has not been proven. Storing internet traffic data is much more difficult than phone data, internet traffic data is far less reliable than phone data, and internet traffic data is far less useful than phone data. Internet data retention is easy to avoid by abusing innocent people. On top of this, the open and decentralized character of the internet is threatened by data retention. And other, more targeted measures are available and waiting to be implemented.

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler, Stavros Lambrinidis et Giovanni Claudio Fava

Amendment 152
Article 4, paragraph 1

Categories of data to be retained	Categories ***and types*** of data to be retained
Member States shall ensure that the following categories of data are retained under this Directive:	***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;	(a) data necessary to trace and identify the source of a communication;
(b) data necessary to trace and identify the destination of a communication;	(b) data necessary to trace and identify the destination of a communication;
(c) data necessary to identify the date, time and duration of a communication;	(c) data necessary to identify the date, time and duration of a communication;
(d) data necessary to identify the type of communication;	(d) data necessary to identify the type of communication;
(e) data necessary to identify the communication device or what purports to be the communication device;	(e) data necessary to identify the communication device or what purports to be the communication device;
(f) data necessary to identify the location of mobile communication equipment.	(f) data necessary to identify the location of mobile communication equipment.
The types of data to be retained under the abovementioned categories of data are specified in the Annex.	***No data revealing the content of the communication can be retained.***

Or. xm

Justification

Amendment by Sylvia-Yvonne Kaufmann

Amendment 153
Article 4, paragraph 1

Member States shall ensure that the	***1.*** Member States shall ensure that the

following categories of data are retained under this Directive:	following categories of data are retained under this Directive:

Or. de

Justification

Follow-up amendment.

Amendment by Herbert Reul

Amendment 154
Article 4, paragraph 1(a)

(a) data necessary to trace and identify the source of a communication***;***	(a) data necessary to trace and identify the source of a communication***:***
	(1) Concerning fixed network telephony:
	(a) the calling telephone number;
	(b) name and address of the subscriber or registered user;
	(2) Concerning mobile telephony:
	(a) the calling telephone number;
	(b) name and address of the subscriber or registered user;
	(3) Concerning Internet access, Internet e-mail and Internet telephony:
	(a) the Internet Protocol (IP) address, whether dynamic or static, allocated by the Internet access provider to a communication;
	(b) the User ID of the source of a communication;
	(c) the Connection Label or telephone number allocated to any communication entering the public telephone network;
	(d) name and address of the subscriber or

registered user to whom the IP address, Connection Label or User ID was allocated at the time of the communication.

Or. de

Justification

The annex should be deleted and incorporated into Article 4. The list of data does not simply represent a detailed technical provision, but is a key provision of the proposal for a directive as a whole. For that reason, it should be incorporated into the operative part of the directive.

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler and Giovanni Claudio Fava

Amendment 155
Article 4, paragraph 2 a (new)

The types of data to be retained shall be as follows:

a) Data necessary to trace and identify the source of a communication:

(1) Concerning fixed network telephony:

(a) the calling telephone number;

(b) the name and address of the subscriber or registered user;

(2) Concerning mobile telephony:

(a) the calling telephone number;

(b) the name and address of the subscriber or registered user;

(3) Concerning Internet

access, Internet e-mail and Internet telephony:

(a) the Internet Protocol (IP) address, whether dynamic or static, allocated by the Internet access provider to a communication;

(b) the user ID of the source of a communication;

(c) the connection label or telephone number allocated to any communication entering the public telephone network;

(d) the name and address of the subscriber or registered user to whom the IP address, connection label or user ID was allocated at the time of the communication.

b) Data necessary to trace and identify the destination of a communication:

Concerning fixed network telephony:

(e) the called telephone number or numbers;

(f) the name(s) and address(es) of the subscriber(s) or registered user(s).

(4) Concerning mobile

telephony:

(a) the called telephone number or numbers;

(b) the name(s) and address(es) of the subscriber(s) or registered user(s).

(5) Concerning Internet access, Internet e-mail and Internet telephony:

(a) the connection label or user ID of the intended recipient(s) of a communication;

(b) the name(s) and address(es) of the subscriber(s) or registered user(s) who is/are the intended recipient(s) of the communication.

c) Data necessary to identify the date, time and duration of a communication:

Concerning fixed network telephony and mobile telephony:

(c) the date and time of the start and end of the communication.

(6) Concerning Internet access, Internet e-mail and Internet telephony:

(a) the date and time of the log-in and log-off of the Internet sessions based on a certain time zone.

d) Data necessary to identify the type

of communication:

Concerning fixed network telephony:

(a) the telephone service used, e.g. voice, conference call, fax and messaging services.

(7) Concerning mobile telephony:

(a) the telephone service used, e.g. voice, conference call, short message service (SMS), enhanced media service (EMS) or multimedia service (MMS).

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

Concerning mobile telephony:

(b) the international mobile subscriber identity (IMSI) of the calling and called party;

(c) the international mobile equipment identity (IMEI) of the calling and called party.

Concerning Internet access, Internet e-mail and Internet telephony:

(d) the calling telephone number for dial-up

access;

(e) the digital subscriber line (DSL) or other end point identifier of the originator of the communication;

(f) the media access control (MAC) address or other machine identifier of the originator of the communication.

f) Data necessary to identify the location of mobile communication equipment:

(1) the local label (cell ID) at the start of the communication;

Or. fr

Amendment by Michael Cashman

Amendment 156
Article 4, paragraph 2 a (new)

Types of data to be retained under the categories identified in this Article:

a) Data necessary to trace and identify the source of a communication:

(1) Concerning Fixed Network Telephony:

(a) The calling telephone number;

(b) Name and address of the subscriber or registered user;

(2) Concerning Mobile Telephony:

(a) The calling telephone number;

(b) Name and Address of the subscriber or registered user;

(3) Concerning Internet Access,

Internet e-mail and Internet telephony:

(a) The Internet Protocol (IP) address, whether dynamic or static, allocated by the Internet access provider to a communication;

(b) The User ID of the source of a communication;

(c) The Connection Label or telephone number allocated to any communication entering the public telephone network;

(d) Name and address of the subscriber or registered user to whom the IP address, Connection Label or User ID was allocated at the time of the communication.

b) Data necessary to trace and identify the destination of a communication:

(1) Concerning Fixed Network Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

(2) Concerning Mobile Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

(3) Concerning Internet Access , Internet e-mail and Internet telephony:

(a) The Connection Label or User ID of the intended recipient(s) of a communication;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s) who are the intended recipient(s) of the communication.

c) Data necessary to identify the date, time and duration of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony:

(a) The date and time of the start and end of the communication.

(2) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The date and time of the log-in and log-off of the Internet sessions based on a certain time zone.

d) Data necessary to identify the type of communication:

(1) Concerning Fixed Network Telephony:

(a) The telephone service used, e.g. voice, conference call, fax and messaging services.

(2) Concerning Mobile Telephony:

(a) The telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service.

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

(1) Concerning Mobile Telephony:

(a) The International Mobile Subscriber Identity (IMSI) of the calling and called party;

(b) The International Mobile Equipment Identity (IMEI) of the calling and called party.

(2) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The calling telephone number for dial-up access;

(b) The digital subscriber line (DSL) or other end point identifier of the originator of the communication;

(c) The media access control (MAC) address or other machine

identifier 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 and end of the communication;

(2) Data mapping between Cell IDs and their geographical location at the start and end of the communication.

Or. en

Justification

This amendment moves the text of the annex of the Commission's proposal into the body of the Directive.

Amendment by Jean-Marie Cavada

Amendment 157
Article 4, introductory part

Member States shall ensure that the following ***categories of data are retained under this Directive***:	***The data necessary are*** the following:

Or. en

Amendment by Jean-Marie Cavada

Amendment 158
Article 4, paragraph 1, point (a)

(a) data necessary to trace and identify the source of a communication***;***	(a) data necessary to trace and identify the source of a communication***:***
	(1) Concerning Fixed and Mobile Telephone Services :
	(a) The calling telephone number;
	(b) Name and address of the subscriber or registered user;
	(2) Concerning Internet Access, Internet e-mail and Internet telephony:
	(a) The Internet Protocol (IP)

address, whether dynamic or static, allocated by the Internet access provider to a communication;

(b) The User ID of the source of a communication;

(c) The Connection Label or telephone number allocated to any communication entering the public telephone network;

(d) Name and address of the subscriber or registered user to whom the IP address, Connection Label or User ID was allocated at the time of the communication;

Or. en

Amendment by Herbert Reul

Amendment 159
Article 4, paragraph 1(b)

(b) data necessary to trace and identify the destination of a communication***;***	(b) data necessary to trace and identify the destination of a communication***:***
	(1) Concerning fixed network telephony:
	(a) the called telephone number or numbers;
	(b) name(s) and address(es) of the subscriber(s) or registered user(s);
	(2) Concerning mobile telephony:
	(a) the called telephone number or numbers;
	(b) Name(s) and address(es) of the subscriber(s) or registered user(s);
	(3) Concerning Internet access, Internet e-mail and Internet telephony:
	(a) the Connection Label or User ID of the intended recipient(s) of a communication;

(b) name(s) and address(es) of the subscriber(s) or registered user(s) who are the intended recipient(s) of the communication.

Or. de

Justification

The annex should be deleted and incorporated into Article 4. The list of data does not simply represent a detailed technical provision, but is a key provision of the proposal for a directive as a whole. For that reason, it should be incorporated into the operative part of the directive.

Amendment by Jean-Marie Cavada

Amendment 160
Article 4, paragraph 1, point (b)

b) data necessary to trace and identify the destination of a communication***;***	b) data necessary to trace and identify the destination of a communication***:***
	(1) Concerning Fixed and Mobile Telephone Services :
	(a) The called telephone number or numbers;
	(b) Name(s) and address(es) of the subscriber(s) or registered user(s);
	(2) Concerning Internet Access, Internet e-mail and Internet telephony:
	(a) The Connection Label or User ID of the intended recipient(s) of a communication;
	(b) Name(s) and address(es) of the subscriber(s) or registered user(s) who are the intended recipient(s) of the communication;

Or. en

Amendment by Jean-Marie Cavada

Amendment 161
Article 4, paragraph 1, point (c)

(c) data necessary to identify the date, time and duration of a communication***;***	(c) data necessary to identify the date, time and duration of a communication: ***(1) Concerning Fixed Network Telephony and Mobile Telephony:*** ***(a) The date and time of the start and end of the communication.*** ***(2) Concerning Internet Access, Internet e-mail and Internet telephony:*** ***(a) The date and time of the log-in and log-off of the Internet sessions based on a certain time zone;***

Or. en

Amendment by Herbert Reul

Amendment 162
Article 4, paragraph 1(c)

(c) data necessary to identify the date, time and duration of a communication***;***	(c) data necessary to identify the date, time and duration of a communication***:*** ***(1) Concerning fixed network telephony and mobile telephony:*** ***(a) the date and time of the start and end of the communication;*** ***(2) Concerning Internet access, Internet e-mail and Internet telephony:*** ***(a) the date and time of the log-in and log-off of the Internet sessions based on a certain time zone.***

Or. de

Justification

The annex should be deleted and incorporated into Article 4. The list of data does not simply

represent a detailed technical provision, but is a key provision of the proposal for a directive as a whole. For that reason, it should be incorporated into the operative part of the directive.

Amendment by Jean-Marie Cavada

Amendment 163
Article 4, paragraph 1, point (d)

(d) data necessary to identify the type of communication***;***	(d) data necessary to identify the type of communication***:***
	(1) Concerning Fixed Network Telephony:
	(a) The telephone service used, e.g. voice, conference call, fax and messaging services.
	(2) Concerning Mobile Telephony:
	(a) The telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service;

Or. en

Amendment by Herbert Reul

Amendment 164
Article 4, paragraph 1(d)

(d) data necessary to identify the type of communication***;***	(d) data necessary to identify the type of communication***:***
	(1) Concerning fixed network telephony:
	(a) the telephone service used, e.g. voice, conference call, fax and messaging services.
	(2) Concerning mobile telephony:
	(a) the telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service.

Or. de

Justification

The annex should be deleted and incorporated into Article 4. The list of data does not simply represent a detailed technical provision, but is a key provision of the proposal for a directive as a whole. For that reason, it should be incorporated into the operative part of the directive.

Amendment by Jean-Marie Cavada

Amendment 165
Article 4, paragraph 1, point (e)

(e) data necessary to identify the communication device or what purports to be the communication device***;***	(e) Data necessary to identify the communication device or what purports to be the communication device***:***
	(1) Concerning Mobile Telephony:
	(a) The International Mobile Subscriber Identity (IMSI) of the calling and called party;
	(b) The International Mobile Equipment Identity (IMEI) of the calling and called party.
	(2) Concerning Internet Access, Internet e-mail and Internet telephony:
	(a) The calling telephone number for dial-up access;
	(b) The digital subscriber line (DSL) or other end point identifier of the originator of the communication;
	(c) The media access control (MAC) address or other machine identifier of the originator of the communication;

Or. en

Amendment by Herbert Reul

Amendment 166
Article 4, paragraph 1(e)

(e) data necessary to identify the	(e) data necessary to identify the

communication device or what purports to be the communication device***;***	communication device or what purports to be the communication device***:***
	(1) Concerning mobile telephony:
	(a) the International Mobile Subscriber Identity.
	(2) Concerning Internet access, Internet e-mail and Internet telephony:
	(a) the calling telephone number for dial-up access;
	(b) the digital subscriber line (DSL) or other end point identifier of the originator of the communication.

Or. de

Justification

The annex should be deleted and incorporated into Article 4. The list of data does not simply represent a detailed technical provision, but is a key provision of the proposal for a directive as a whole. For that reason, it should be incorporated into the operative part of the directive.

Manufacturers allocate the same serial number to several mobile phones, making manipulation by users easy.

The device number of a computer network card cannot be reliably matched to an individual, since such numbers are likewise allocated several times over by manufacturers and can easily be manipulated by users. The retention of both these data types can make no tangible contribution to fighting crime.

Amendment by Jean-Marie Cavada

Amendment 167
Article 4, paragraph 1, point (f)

(f) data necessary to identify the location of mobile communication equipment**.**	(f) data necessary to identify the location of mobile communication equipment***:***
	(1) The location label (Cell ID) at the start and end of the communication;

Or. en

Amendment by Charlotte Cederschiöld

Amendment 168
Article 4, paragraph 1, point f)

f) data necessary to identify the location of mobile communication equipment.	***deleted***

Or. en

Justification

...

Amendment by Herbert Reul

Amendment 169
Article 4, paragraph 1(f)

(f) data necessary to identify the location of mobile communication equipment.	(f) data necessary to identify the location of mobile communication equipment***:***
	(1) the location label (Cell ID) at the start of the communication.

Or. de

Justification

The annex should be deleted and incorporated into Article 4. The list of data does not simply represent a detailed technical provision, but is a key provision of the proposal for a directive as a whole. For that reason, it should be incorporated into the operative part of the directive. Manufacturers allocate the same serial number to several mobile phones, making manipulation by users easy. At present, in the area of mobile telephony only location data at the start of a mobile telephony communication are retained. The proposal that location data at the end of a mobile telephony communication should be retained would generate high investment costs out of all proportion to the likely value of such data as an investigatory tool for the law enforcement authorities.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 170
Article 4(f)

(f) data necessary to identify the location of mobile communication equipment.	***Deleted***

Or. de

Justification

The retention of location data would make it possible to draw up and retain comprehensive movement profiles for every EU citizen.

Amendment by Jean-Marie Cavada

Amendment 171
Article 4, paragraph 2

The types of data to be retained under the abovementioned categories of data are specified in the Annex.	***Specific guarantees will be provided for in order to ensure a stringent, effective distinction between content and traffic data, both for the Internet and for telephony.***

Or. en

Amendment by Herbert Reul

Amendment 172
Article 4, paragraph 2

The types of data to be retained under the abovementioned categories of data are specified in the Annex.	***Member States shall be free to retain other*** types of data***, e.g. unsuccessful attempts to secure a connection, within these*** categories of data.

Or. de

Justification

The annex should be deleted and incorporated into Article 4. The list of data does not simply represent a detailed technical provision, but is a key provision of the proposal for a directive as a whole. For that reason, it should be incorporated into the operative part of the directive. An opt-clause would enable Member States to retain more data if they feel such a step is necessary to safeguard their national security.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 173
Article 4, paragraph 2 a (new)

The following types of data shall be retained under the categories identified in paragraph 1:

(a) data necessary to trace and identify the source of a communication:

(1) concerning fixed network telephony:

(a) the calling telephone number;

(b) the name and address of the subscriber or registered user;

(2) concerning mobile telephony:

(a) the calling telephone number;

(b) the name and address of the subscriber or registered user;

(b) data necessary to trace and identify the destination of a communication:

(1) concerning fixed network telephony:

(a) the telephone number(s) called;

(b) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning mobile telephony:

(a) the telephone number(s) called;

(b) the name(s) and address(es) of the subscriber(s) or registered user(s);

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony:

(a) the date and the exact time of the start and end of the communication;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony:

(a) the telephone service used, e.g. voice telephony, conference call,

fax, messaging services;

(2) concerning mobile telephony:

(a) the mobile telephony service used, e.g. voice telephony, conference call, short message service, enhanced media service or multi-media service;

(e) data necessary to identify the communication device or what purports to be the communication device:

(1) concerning mobile telephony:

(a) the international mobile subscriber identity (IMSI) of the calling and called party;

(b) the international mobile equipment identity (IMEI) of the calling and called party.

Or. de

Justification

Provisions governing matters as central to the fundamental rights of European citizens as the retention of personal data should not be amended under the comitology procedure, but only with Parliament's involvement.

Amendment by Jean-Marie Cavada, Kathalijne Maria Buitenweg, Charlotte Cederschiöld, Edith Mastenbroek, Lilli Gruber, Herbert Reul, Sylvia-Yvonne Kaufmann, Martine Roure,Wolfgang Kreissl-Dörfler

Amendments 174 to 180
Article 5

Revision of the annex	***deleted***
The Annex shall be revised on a regular basis as necessary in accordance with the procedure referred to in Article 6(2).	

Or. en

Amendment by Jean-Marie Cavada

Amendment 181
Article 5

The ***Annex*** shall be revised on a regular basis ***as necessary in accordance with the procedure referred to in Article 6(2).***	The ***list of data*** shall be revised on a regular basis.

Or. en

Amendment by Herbert Reul, Kathalijne Maria Buitenweg, Charlotte Cederschiöld, Edith Mastenbroek, Lilli Gruber, Martine Roure and Wolfgang Kreissl-Dörfler

Amendments 182 to 186
Article 6

Article 6	***Deleted***
Committee	
1. The Commission shall be assisted by a Committee composed of representatives of the Member States and chaired by the representative of the Commission.	
2. Where reference is made to this paragraph, Article 5 and 7 of Decision 1999/468/EC shall apply, having regard to the provisions of Article 8 thereof.	
3. The period laid down in Article 5(6) of Decision 1999/468/EC shall be three months.	

Or. de

Justification

It is unacceptable that the comitology procedure should be used to amend the lists of data types set out in the annex. Since this is a matter central to citizens' fundamental rights, Parliament must be involved.

Amendment by Herbert Reul

Amendment 187
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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***.	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***six months*** from the date of the communication***. However, Member States shall be free to retain the categories of data referred to in Article 4 for a longer period***.

Or. de

Justification

On the basis of empirical studies, the six-month retention period covers most of the law enforcement authorities' needs as regards Internet and telephone data.

The opt-out clause would enable Member States to retain data for a longer period if they feel such a step is necessary to safeguard their national security.

Amendment by Sylvia-Yvonne Kaufmann

Amendment 188
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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***.	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***three months*** from the date of the communication***. Thereafter, the data must be erased, unless there is sufficient evidence to suspect that the subscriber or registered user has committed a criminal offence***.

Or. de

Justification

The aim of this amendment is to keep data retention to a minimum and, at the same time, in line with the needs of the law enforcement authorities, to provide for the retention of data, under certain circumstances, for periods in excess of three months. The combination of data retention and quick freeze will extend the scope of the directive to other data relating to flat-rate users for the first time, thereby meeting the needs of the law enforcement authorities. The

shortness of the retention period will minimise the impact on fundamental and human rights.

Amendment by Martine Roure and Wolfgang Kreissl-Dörfler

Amendment 189
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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.	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***six months up to a maximum of two years*** 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. ***Member States shall ensure that all data is erased at the end of this retention period***.

Or. fr

Amendment by Sarah Ludford

Amendment 190
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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.***	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***6 months*** from the date of the communication**.**

Or. en

Justification

The simple fact of retaining traffic data for longer periods (12 months as proposed by the Draft Directive) will only produce more data volumes, without proportionally increasing the quality of information. Larger volumes of data also increase the complexity of the translation of data into information and the risks of misuses and the need for increased security. LEAs will have to optimise ICT resources in order to request more precise and accurate data.

So far, LEAs have not been able to justify a general minimum data retention period that exceeds 6 months. On the contrary, empirical data shows that a 6 month retention period already covers the majority of public authorities' needs. Even the President of the Federal Criminal Police Office considers a preservation period of 6 months to be fully sufficient. The experiences of other EU Member States also show that, as for example in Sweden, 85% of the data requested is not more than 3 months old. In the UK, too, providers estimate that 80% of requests for information relate to data that is less than 3 months old.

The retention periods should be kept to the absolute minimum in order to minimize the complexity for retrieving information out of the available data.

Amendment by Stavros Lambrinidis

Amendment 191
Article 7 a (new)

Article 7a
Data protection and data security

Each Member State shall ensure that data retained under this Directive is subject, as a minimum, to the rules implementing Article 16 and 17 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movements of such data, to the provisions of Article 4 and 5 of Directive 2002/58/EC and the following data security principles:
a) the data shall be subject to appropriate security measures to protect it against accidental or unlawful destruction, loss, or alteration;
b) providers of publicly available electronic communications services or networks as well as Member State authorities accessing the data shall take the appropriate security measures to prevent unauthorized or other inappropriate or unlawful storage, access, processing, disclosure, or use, including through fully updated technical systems to protect the integrity of data and through the designation of specially authorized personnel who can have exclusive access to the data;
c) providers of publicly available electronic communications services or networks

create a separate system of storage of data for public order purposes, the data of this separate system cannot under any circumstance be used for business purposes or other purposes not explicitly authorized under this Directive,
d) the data cannot under any circumstances be transmitted to third countries and third parties,
e) an appropriate independent authority in each Member State is designated to oversee the lawful implementation of this Directive regarding the security of the stored data as well as in each case where data is requested, accessed, processed and used, subject to the overall oversight authority of national legislatures.

Or. en

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler, Stavros Lambrinidis et Giovanni Claudio Fava

Amendment 192
Article 7 a (new)

Article 7a
Data protection and data security

Each Member State shall ensure that data retained under this Directive is subject, as a minimum, to the rules implementing Article 16 and 17 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movements of such data, to the provisions of Article 4 and 5 of Directive 2002/58/EC and the following data security principles:
a) the data shall be subject to appropriate security measures to protect it against accidental or unlawful destruction, loss, or alteration;
b) providers of publicly available electronic communications services or networks as well as Member State authorities accessing the data shall take the appropriate security measures to prevent unauthorized or other

inappropriate or unlawful storage, access, processing, disclosure, or use, including through fully updated technical systems to protect the integrity of data and through the designation of specially authorized personnel who can have exclusive access to the data;
c) providers of publicly available electronic communications services or networks create a separate system of storage of data for public order purposes, the data of this separate system cannot under any circumstance be used for business purposes;
d) the data can only be transmitted to third countries and third parties under special circumstances,
e) an appropriate independent authority in each Member State is designated to oversee the lawful implementation of this Directive regarding the security of the stored data as well as in each case where data is requested, accessed, processed and used, subject to the overall oversight authority of national legislatures.

Or. xm

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 193 to 196
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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.***	***1.*** Member States shall ensure that the categories ***and types*** of data referred to in Article 4 are retained for a period of ***six months*** from the date of the communication. ***After this period has elapsed, the retained data have to be deleted.***
	2. By derogation from paragraph 1, any Member State may provide for retention of communication data referred to in Article 4 for longer periods in accordance with national criteria, following national

procedural or consultative processes, when such retention constitutes a necessary, appropriate and proportionate measure within a democratic society.

3. By derogation from paragraph 1, any Member State may provide for retention of communication data referred to in Article 3 for shorter periods should the Member State not find acceptable, following national procedural or consultative processes, the retention periods set out in paragraph 1 of this Article as well as in Article 3.

4. Any Member State making use of paragraphs 2 or 3 must notify the Council and the Commission. Any such derogation must be evaluated every 2 years.

Or. en

Amendment by Jean-Marie Cavada

Amendment 197
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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.	Member States shall ensure that the categories of data referred to in Article 4 are retained ***no longer than*** 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 ***maximum*** period of 6 months. ***Members States shall ensure that all the data are erased at the end of the retention period.***

Or. en

Amendment by Bill Newton Dunn

Amendment 198
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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.***	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of one year from the date of the communication**.**

Or. en

Amendment by Kathalijne Maria Buitenweg

Amendment 199
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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.***	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***three months*** from the date of the communication.

Or. en

Amendment by Charlotte Cederschiöld

Amendment 200
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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.	Member States shall ensure that the categories of data referred to in Article 4, ***paragraph 1 (a-e)*** are retained for a ***harmonised*** period of ***three months*** from the date of the communication. ***Should the evaluation in Article 12 demonstrate a need for necessary and proportionate changes in the retention period adjustments could be made if***

harmonised.

Or. en

Amendment by Ioannis Varvitsiotis

Amendment 201
Article 7

Member States shall ensure that the categories of data referred to in Article 4 are 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***.	Member States shall ensure that the categories of data referred to in Article 4 are retained for a period of ***six months*** 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 ***three months***.

Or. en

Justification

In view of the cost and the use of the data, we support a shorter period of data retention.

Amendment by Jean-Marie Cavada

Amendment 202
Article 7, paragraph 1 a (new)

By derogation from paragraph 1, Member States may provide for the retention of data for longer periods, when such retention constitutes, given the particular situation in a Member State, a necessary, appropriate and proportionate measure within a democratic society. The procedure of Article 95, paragraphs 4 and following, applies.

Or. en

Amendment by Herbert Reul

Amendment 203
Article 8

Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay.	Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent ***law enforcement*** authorities ***of the Member States concerned*** without undue delay. ***A judicial ruling shall be required before data is transmitted.***

Or. de

Justification

The wording of this provision must define more clearly which authorities in the Member States may have access to retained data. In order to ensure that retained data is not misused, a judicial ruling should be handed down before data is transmitted to law enforcement authorities.

Amendment by Ioannis Varvitsiotis

Amendment 204
Article 8

Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay.	Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent ***national*** authorities without undue delay***, following the approval of the judicial authorities***.

Or. en

Justification

There must be a judicial control to the access to the data.

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 205
Article 8

Storage requirements for retained data	***Processing of*** data
Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay.	Member States shall ensure that the data are retained in accordance with this Directive in such a way that the data retained and any other necessary information related to such data can be transmitted upon request to the competent authorities without undue delay. ***The processing of the data takes place in accordance with the provisions of Article 17 of Directive 95/46/EC and Article 4 of Directive 2002/58/EC.***

Or. en

Amendment by Jean-Marie Cavada

Amendment 206
Article 8

Member States shall ensure that the data are retained in accordance with this Directive in such a way that ***the data retained and any other necessary information related to such data*** can be transmitted upon request to the competent authorities without undue delay.	Member States shall ensure that the data ***as specified in Article 4*** are retained ***by providers of publicly available electronic communications services or of a public communicating network,*** in accordance with this Directive, in such a way that they can be transmitted upon request to the competent authorities without undue delay. ***Only well trained members of the staff with specified technical responsibilities can have access to the data.*** ***Specific rules on confidentiality must be provided for. Logging of each access must be ensured and systematic auditing performed and kept at disposal of the national data protection authorities.***

Or. en

Amendment by Charlotte Cederschiöld

Amendment 207
Article 8

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

Or. en

Justification

See Art 2 paragraph 2 point bb

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler, Stavros Lambrinidis and Giovanni Claudio Fava

Amendment 208
Article 8 a (new)

	Article 8a
	Penalties
	Member States shall take the necessary measures to ensure that any improper or negligent use of or access to data in violation of the provisions of this Directive is punishable by effective, proportionate and dissuasive criminal penalties.

Or. fr

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 209
Article 9

Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the European Commission on a yearly basis.	Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the European Commission on a yearly basis. ***The European Commission shall forward***

	the statistics to the European Parliament.
Such statistics shall include	Such statistics shall include
- the cases in which information has been provided to the competent authorities in accordance with applicable national law,	– the cases in which information has been provided to the authorities***, including intelligence and security services,*** 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 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.	– the cases where requests for data could not be met.
	- the (positive or negative) outcome of investigations in which information has been used, as well as estimates regarding the necessity of the information for the investigation.
Such statistics shall not contain personal data.	Such statistics shall not contain personal data.

Or. en

Amendment by Sylvia-Yvonne Kaufmann

Amendment 210
Article 9

Member States shall ensure that statistics on the retention of data processed in connection with the provision of ***public*** electronic communication services are provided to the European Commission on a yearly basis. Such statistics shall include	Member States shall ensure that statistics on the retention of data processed in connection with the provision of ***publicly available*** electronic communication services are provided to the European Commission on a yearly basis. Such statistics shall include
- the cases in which information has been provided to the competent authorities in accordance with applicable national law,	- the cases in which information has been 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 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***.	- the ***number of*** cases where ***the data requested did not directly lead to the successful conclusion of the relevant***

	investigations;
	- the number of cases where data requested was not available to the undertakings concerned.
	The European Commission shall submit these statistics to the European Parliament each year.
Such statistics shall not contain personal data.	Such statistics shall not contain personal data.

Or. de

Justification

Proper statistics are needed if a detailed analysis is to be carried out to determine whether the retention of traffic data is a worthwhile measure justifying such a far-reaching encroachment on citizens' fundamental rights.

Amendment by Herbert Reul

Amendment 211
Article 9

Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the European Commission on a yearly basis. Such statistics shall include	Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the European Commission on a yearly basis. Such statistics***, to be drawn up by the law enforcement authorities,*** shall include
- the cases in which information has been provided to the competent authorities in accordance with applicable national law,	- the cases in which information has been 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 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.	- the cases where requests for data could not be met***;***
	- the number of cases where given types of data have led or made a significant contribution to the successful conclusion of an investigation.
Such statistics shall not contain personal	Such statistics shall not contain personal

data.	data.

Or. de

Justification

The directive should require law enforcement authorities to draw up the statistics in question.

The proposed measures alone make little sense, since the number of requests and the age of the data concerned are hardly enough to demonstrate the value of data retention. It is essential that the law enforcement authorities should show in how many cases given types of data of a given age have actually led or made a significant contribution to the successful conclusion of an investigation.

Amendment by Stavros Lambrinidis

Amendment 212
Article 9

Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the European Commission on a yearly basis. Such statistics shall include – the cases in which information has been 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.	Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the European Commission on a yearly basis. Such statistics shall include – the cases in which information has been 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. ***- the cases where the provided data proved either not helpful or not necessary for the prevention, detection, investigation or prosecution of specific crimes for which it was accessed under this Directive.*** Such statistics shall not contain personal data.

Or. en

Justification

To determine whether the measures included in the Directive remain necessary and effective during future reviews, it is important that the statistics kept address these issues. In this regard, it is reminded that the Presidency of the Council, in its recent Paper entitled "Liberty and Security: Striking the Right Balance," noted that, "in the future some criminals and terrorists will adapt their use of technology to make the retention of data a less important tool for investigations."

Amendment by Jean-Marie Cavada

Amendment 213
Article 9, paragraph 1, introductory part

Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the European Commission on a yearly basis. Such statistics shall include	Member States shall ensure that statistics on the retention of data processed in connection with the provision of public electronic communication services are provided to the European Commission on a yearly basis. ***ENISA may provide help to Member States in collecting these statistics.*** Such statistics shall include

Or. en

Amendment by Charlotte Cederschiöld

Amendment 214
Article 9, paragraph 1, indent 3 a (new)

	- the cases where suspected and factual security breaches occurred.

Or. en

Justification

As risks are substantial with large and complex data retention systems it is crucial to include statistics on suspected and factual security breaches.

Amendment by Charlotte Cederschiöld

Amendment 215
Article 9 a (new)

	Article 9a
	Each Member State shall nominate one independent official responsible directly to the European Data Protection Supervisor and the Commission to report the above stated statistics on a yearly basis.

Or. en

Amendment by Michael Cashman

Amendment 216
Article 10

Costs	***deleted***
Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	

Or. en

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler and Giovanni Claudio Fava

Amendment 217
Article 10

Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive***, including the additional costs of data protection.***

Or. fr

Amendment by Sarah Ludford

Amendment 218
Article 10

Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are ***fully*** reimbursed for demonstrated additional ***investment and operating*** costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive ***and any future amendments to it. The reimbursement should include costs arising from making the retained data available to law enforcement authorities.***

Or. en

Justification

This Directive does not merely regulate how communications service providers operate, it imposes a duty upon them to do undertake costly work specifically for law enforcement purposes. Most of those costs will probably be passed on to costumers.

It needs to be clearly understood that if law enforcement require access to data that is only retained as a result of this Directive, the cost of satisfying that demand (changes in systems' design, increased storage capacity, additional security measures, verification and responses to access requests, retrieval of raw data etc) is also a consequence of this Directive.

A cost-based access charge also tends to impose a certain restraint and discipline in limiting the number and scope of requests to what is actually needed for law enforcement purposes.

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 219
Article 10

Member States shall ensure that providers of publicly available ***electronic*** communication services or of a public communication network are reimbursed for demonstrated	Member States shall ensure that providers of publicly available communication services or of a public communication network are reimbursed for demonstrated additional costs

additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	they have incurred in order to comply with obligations imposed on them as a consequence of this Directive. ***In addition, Member States shall set up a uniform fee system for every request a law enforcement authority makes.***

Or. en

Amendment by Bill Newton Dunn

Amendment 220
Article 10

Member States shall ***ensure that*** providers of publicly available electronic communication services or of a public communication network ***are reimbursed*** for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	Member States shall ***provide for reimbursement to*** providers of publicly available electronic communication services or of a public communication network for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.

Or. en

Justification

Member States should provide for reimbursement to the services providers for the demonstrated additional costs that they have incurred when complying with the obligation to retain data.

Amendment by Charlotte Cederschiöld

Amendment 221
Article 10

Member States ***shall*** ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	Member States ***shall*** ensure that providers of publicly available electronic communication services or of a public communication network are ***fully*** reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.

Or. en

Amendment by Herbert Reul

Amendment 222
Article 10

Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.	Member States shall ensure that providers of publicly available electronic communication services or of a public communication network are ***fully*** reimbursed for demonstrated additional costs they have incurred in order to comply with obligations imposed on them as a consequence of this Directive.

Or. de

Justification

It must be made clear that Member States will reimburse to undertakings the full costs generated by data retention, since the fight against crime is a task for the public authorities.

Amendment by Charlotte Cederschiöld

Amendment 223
Article 11

In Article 15 of Directive 2002/58/EC the following paragraph 1a is inserted:	***deleted***
”1a. Paragraph 1 shall not apply to obligations relating to the retention of data for the prevention, investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, deriving from Directive 2005/../EC*. * OJ L nr. …. of ….”.	

Or. en

Justification

The purpose of this Article is to amend an other Directive (2002/58/EC) via this Directive and add possibilities to deviate from the original requirements that all data retention must be ”appropriate, proportionate and necessary”.

Amendment by Jean-Marie Cavada

Amendment 224
Article 11

In Article 15 of Directive 2002/58/EC the following paragraph 1a is inserted:	In Article 15 of Directive 2002/58/EC the following paragraph 1a is inserted:
”1a. Paragraph 1 shall not apply to obligations relating to the retention of data for the ***prevention,*** investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, deriving from Directive 2005/../EC*. * OJ L nr. …. of ….”.	"1a. Paragraph 1 shall not apply to obligations relating to the retention of data for the investigation, detection and prosecution of serious criminal offences, such as terrorism and organised crime, deriving from ***the transposition of*** Directive 2005/../EC. * * OJ L nr. ..... of .....
	Member States shall refrain from adopting legislative measures in the sectors covered by this Directive.

Or. en

Amendment by Herbert Reul

Amendment 225
Article 12, paragraph 1

1. Not later than ***three*** years from the date referred to in Article 13(1), 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 the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to the period of retention provided for in Article 7.	1. Not later than ***two*** years from the date referred to in Article 13(1), 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 the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to the period of retention provided for in Article 7 ***and the types of data specified in Article 4(1)***.

Or. de

Justification

Not only the retention period, but also individual types of data, must be assessed as to their relevance in the fight against crime.

Amendment by Jean-Marie Cavada

Amendment 226
Article 12, paragraph 1

1. Not later than ***three*** years from the date referred to in Article 13(1), 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 the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to the period of retention provided for in Article 7.	1. Not later than ***two*** years from the date referred to in Article 13(1) ***and in the light of the expiration of the retention measures adopted by Member States on the basis of this Directive***, the Commission shall submit to the European Parliament and the Council an evaluation of ***the effectiveness of the provisions contained in the Directive, and of the*** impact on ***fundamental rights of the data subjects. The evaluation will also considers the impact of the measures on*** economic operators and consumers, taking into account the statistical elements provided to the Commission pursuant to Article 9. ***The results of the evaluations will be publicly available.***

Or. en

Amendment by Edith Mastenbroek and Lilli Gruber

Amendment 227
Article 12, paragraph 1

1. Not later than ***three years*** from the date referred to in Article 13(1), 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 the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive***, in particular with regard to the period of retention provided for in Article 7.***	1. Not later than ***two years*** from the date referred to in Article 13(1), 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. ***The Commission shall also report on the necessity and effectiveness of this directive, as well as its impact on fundamental rights and privacy,*** taking into account the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of

this Directive.

Or. en

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler and Stavros Lambrinidis

Amendment 228
Article 12, paragraph 1

1. Not later than ***three*** years from the date referred to in Article 13(1), 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 the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to the period of retention provided for in Article 7.	1. Not later than ***two*** years from the date referred to in Article 13(1), the Commission shall submit to the European Parliament and the Council an evaluation of ***the effectiveness of the*** application of this Directive and its impact on economic operators and consumers, taking into account the statistical elements provided to the Commission pursuant to Article 9 with a view to determining whether it is necessary to modify the provisions of this Directive, in particular with regard to the period of retention provided for in Article 7.

Or. fr

Amendment by Jean-Marie Cavada

Amendment 229
Article 12, paragraph 1 a (new)

	1a. The Commission will submit a new Proposal for a Directive, in particular with regard to the types of data and the period of retention, on the basis of the evaluation.

Or. en

Amendment by Martine Roure,Wolfgang Kreissl-Dörfler and Stavros Lambrinidis

Amendment 230
Article 12, paragraph 2

2. To that end, the Commission shall examine all observations communicated to it by the Member States or by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.	2. To that end, the Commission shall examine all observations communicated to it by the Member States***, the European Data Protection Supervisor*** or the Working Party on the Protection of Individuals with regard to the Processing of Personal Data instituted by Article 29 of Directive 95/46/EC.

Or. fr

Amendment by Stavros Lambrinidis, Edith Mastenbroek

Amendment 231
Article 14

This Directive shall enter into force ***on the twentieth day following that of its publication in the Official Journal of the European Union.***	This Directive shall enter into force ***after its publication in the Official Journal of the European Union and upon the entry into force of a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.***

Or. en

Justification

During its presentations to the LIBE Committee, the European Commission repeatedly expressed the view that the protection of data under the present Directive can be fully guaranteed only under a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Amendment by Herbert Reul

Amendment 232
Article 14 a (new)

Article 14a
Revision
No later than two years after the date referred to in Article 13(1), this Directive shall be revised in accordance with the procedure laid down in Article 251 of the EC Treaty. In particular, the types of data

retained and the retention periods shall be assessed to determine their relevance to the fight against terrorism and organised crime in the light of the statistics compiled pursuant to Article 9.

Or. de

Justification

The most important provisions of this directive relate to the types of data which must be retained. In view of their significant technological components, after a relatively short period has elapsed data should be assessed to determine its relevance to the fight against crime. The proposed retention period must be assessed in the same way. Given the scope for violating fundamental rights, Parliament must be involved under the codecision procedure.

Amendment by Jean-Marie Cavada, Kathalijne Maria Buitenweg, Edith Mastenbroek, Lilli Gruber, Sylvia-Yvonne Kaufmann, Herbert Reul, Martine Roure,Wolfgang Kreissl-Dörfler, Stavros Lambrinidis

Amendment 233 to 238
Annex

Types of data to be retained under the categories identified in Article 4 of this Directive:	***deleted***
a) Data necessary to trace and identify the source of a communication:	
(1) Concerning Fixed Network Telephony:	
(a) The calling telephone number;	
(b) Name and address of the subscriber or registered user;	
(2) Concerning Mobile Telephony:	
(a) The calling telephone number;	
(b) Name and Address of the subscriber or registered user;	
(3) Concerning Internet Access, Internet e-mail and Internet telephony:	
(a) The Internet Protocol (IP) address, whether dynamic or	

static, allocated by the Internet access provider to a communication;

(b) The User ID of the source of a communication;

(c) The Connection Label or telephone number allocated to any communication entering the public telephone network;

(d) Name and address of the subscriber or registered user to whom the IP address, Connection Label or User ID was allocated at the time of the communication.

b) Data necessary to trace and identify the destination of a communication:

(1) Concerning Fixed Network Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

(2) Concerning Mobile Telephony:

(a) The called telephone number or numbers;

(b) Name(s) and address(es) of the subscriber(s) or registered user(s);

(3) Concerning Internet Access , Internet e-mail and Internet telephony:

(a) The Connection Label or User ID of the intended recipient(s) of a communication;

(b) Name(s) and address(es) of the subscriber(s) or registered

user(s) who are the intended recipient(s) of the communication.

c) Data necessary to identify the date, time and duration of a communication:

(1) Concerning Fixed Network Telephony and Mobile Telephony:

(a) The date and time of the start and end of the communication.

(2) Concerning Internet Access, Internet e-mail and Internet telephony:

(b) The date and time of the log-in and log-off of the Internet sessions based on a certain time zone.

d) Data necessary to identify the type of communication:

(1) Concerning Fixed Network Telephony:

(a) The telephone service used, e.g. voice, conference call, fax and messaging services.

(2) Concerning Mobile Telephony:

(a) The telephone service used, e.g. voice, conference call, Short Message Service, Enhanced Media Service or Multi-Media Service.

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

(1) Concerning Mobile Telephony:

(a) The International Mobile Subscriber Identity (IMSI) of the calling and called party;

(b) The International Mobile Equipment Identity (IMEI) of the calling and called party.

(2) Concerning Internet Access, Internet e-mail and Internet telephony:

(a) The calling telephone number for dial-up access;

(b) The digital subscriber line (DSL) or other end point identifier of the originator of the communication;

(c) The media access control (MAC) address or other machine identifier 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 and end of the communication;

(2) Data mapping between Cell IDs and their geographical location at the start and end of the communication.

Or. en