EUROPEAN COMMISSION

Brussels, 18.4.2011
COM(2011) 225 final

REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

Evaluation report on the Data Retention Directive (Directive 2006/24/EC)

REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

Evaluation report on the Data Retention Directive (Directive 2006/24/EC)

1. INTRODUCTION

The Data Retention Directive[1] (hereafter 'the Directive') requires Member States to oblige providers of publically available electronic communications services or of public communications networks (hereafter, 'operators') to retain traffic and location data for between six months and two years for the purpose of the investigation, detection and prosecution of serious crime.

This report from the Commission evaluates, in accordance with Article 14 of the Directive, its application by Member States and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and statistics provided to the Commission, with a view to determining whether it is necessary to amend its provisions, in particular with regard to its data coverage and retention periods. This report also examines the implications of the Directive for fundamental rights, in view of the criticisms which have been levelled in general at data retention, and examines whether measures are needed to address concerns associated with the use of anonymous SIM cards for criminal purposes[2].

Overall, the evaluation has demonstrated that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU. The contribution of the Directive to the harmonisation of data retention has been limited in terms of, for example, purpose limitation and retention periods, and also in the area of reimbursement of costs incurred by operators, which is outside its scope. Given the implications and risks for the internal market and for the respect for the right to privacy and the protection of personal data, the EU should continue through common rules to ensure that high standards for the storage, retrieval and use of traffic and location data are consistently maintained. In the light of these conclusions, the Commission intends to propose amendments to the Directive, based on an impact assessment.

2. BACKGROUND TO THIS EVALUATION

This evaluation report has been informed by extensive discussions with and input from Member States, experts and stakeholders.

---

1 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54-63

2 Council conclusions on combating the criminal misuse and anonymous use of electronic communications, 2908th Justice and Home Affairs Council meeting - Brussels, 27-28 November 2008

In May 2009 the Commission hosted a conference entitled 'Towards the Evaluation of the Data Retention Directive' which was attended by data protection authorities, the private sector, civil society and academia. In September 2009, the Commission sent a questionnaire to stakeholders from these groups, to which it received around 70 replies[3]. The Commission hosted a second conference in December 2010, 'Taking on the Data Retention Directive', which was attended by a similar range of stakeholders, to share preliminary assessments of the Directive and to discuss future challenges in the area.

The Commission met representatives of each Member State and associated European Economic Area country between October 2009 and March 2010 to discuss in further detail issues concerning the application of the Directive. Member States started applying the Directive later than expected, particularly with regard to internet-related data. The delays in transposition meant that nine Member States were able, for either 2008 or 2009, to provide the Commission with the full statistics required by Article 10 of the Directive, although overall 19 Member States provided some statistics (see Section 4.7). The Commission wrote to Member States in July 2010 requesting further quantitative and qualitative information pertaining to the necessity of retained data in leading to law enforcement results. Ten Member States responded with details of specific cases for which data proved necessary[4].

This report draws from the position papers adopted, since its establishment in 2008, by the 'Platform on Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime'[5]. The Commission has taken into consideration the reports of the Article 29 Data Protection Working Party[6], and particularly the report on the second enforcement action, that is, its assessment of Member States' compliance with the data protection and data security requirements of the Directive[7].

3. DATA RETENTION IN THE EUROPEAN UNION

3.1. Data retention for criminal justice and law enforcement purposes

Service and network providers (hereafter, 'operators'), in the course of their activities, process personal data for the purpose of transmitting a communication, billing, interconnection payments, marketing and certain other value-added services. Such processing involves data

---

3 Responses have been published on the Commission website (http://ec.europa.eu/home-affairs/news/consulting_public/consulting_0008_en.htm_

4 Belgium, Czech Republic, Cyprus, Lithuania, Hungary, Netherland, Poland, Slovenia, United Kingdom. Sweden also reported several cases of specific serious crimes in which historic traffic data, which was available despite the absence of a data retention obligation, was crucial in securing convictions.

5 This expert group was established under Commission Decision 2008/324/EC, OJ L 111, 23.04.2008, p. 11-14. The Commission has met with the group regularly. Its position papers are published on http://ec.europa.eu/justice_home/doc_centre/police/doc_police_intro_en.htm

6 The Working Party on the Protection of Individuals with regard to the Processing of Personal Data was established pursuant to Article 29 of the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

7 Report 01/2010 on the second joint enforcement action: Compliance at national level of telecom providers and internet service providers with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive' (WP 172), 13.07.2010 (see http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm).

indicating the source, destination, date, time, duration and type of a communication, as well as users' communication equipment and, in the case of mobile telephony, data on the location of equipment. Under Directive 2002/58/EC on privacy in electronic communications (hereafter, 'the e-Privacy Directive')[8], such traffic data generated by the use of electronic communications services must in principle be erased or made anonymous when those data are no longer needed for the transmission of a communication, except where, and only for so long as, they are needed for billing purposes, or where the consent of the subscriber or user has been obtained. Location data may only be processed if they are made anonymous or with the consent of the user concerned, to the extent and for the duration necessary for the provision of a value-added service.

Prior to the entry into force of the Directive, subject to specific conditions, national authorities would request access to such data from operators, in order for example to identify subscribers using an IP address, to analyse communications activities and to identify the location of a mobile phone.

At EU level, the retention and use of data for law enforcement purposes was first addressed by Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector. This Directive first provided for the possibility for Member States to adopt such legislative measures where necessary for the protection of public security, defence or public order, including the economic well-being of the state when the activities related to state security matters and for the enforcement of criminal law[9].

That provision was further developed in the e-Privacy Directive which provides for the possibility for Member States to adopt legislative measures derogating from the principle of confidentiality of communications, including under certain conditions the retention of, and access to and use of, data for law enforcement purposes. Article 15(1) allows Member States to restrict privacy rights and obligations, including through the retention of data for a limited period, where 'necessary, appropriate and proportionate in a democratic society to safeguard national security (i.e. state security), defence, public security and the prevention, investigation, detection and prosecution of criminal offences or of the unauthorised use of the electronic communication system'.

The role of retained data in criminal justice systems and law enforcement is further discussed in section 5.

3.2. The aim and legal basis of the Data Retention Directive

As a consequence of the provisions of Directive 97/66/EC and the e-Privacy Directive, which permit Member States to adopt legislation on data retention, operators in some Member States were required to purchase data retention equipment and employ personnel to retrieve data on behalf of law enforcement authorities, while those in other Member States were not, leading

---

8 Directive of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31/07/2002, p. 0037 – 0047).

9 Article 14(1) of Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30.1.1998, p. 1–8);

to distortions in the internal market. Furthermore, trends in business models and service offerings, such as the growth in flat rate tariffs, pre-paid and free electronic communications services, meant that operators gradually stopped storing traffic and location data for billing purposes thus reducing the availability of such data for criminal justice and law enforcement purposes. The terrorist attacks in Madrid in 2004 and in London in 2005 added urgency to the discussions at EU-level on how to address these issues.

Against that background, the Data Retention Directive imposed on Member States an obligation for providers of publicly available electronic communications services and public communication networks to retain communications data for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in national law, and sought to harmonise across the EU certain related issues.

The Directive amended Article 15(1) of the e-Privacy Directive by adding a paragraph stipulating that Article 15(1) does not apply to data retained under the Data Retention Directive[10]. Therefore, Member States (as stated in Recital 12 of the Directive) continue to be able to derogate from the principle of confidentiality of communications. The (Data Retention) Directive governs only the retention of data for the more limited purpose of investigating, detecting and prosecuting serious crime.

This complex legal relationship between the Directive and the e-Privacy Directive, combined with the absence of a definition in either of the two directives of the notion of 'serious crime', makes it difficult to distinguish, on the one hand, measures taken by Member States to transpose the data retention obligations laid down in the Directive and, on the other, the more general practice in Member States of data retention permitted by Article 15(1) of the e-Privacy Directive[11]. This is discussed further in Section 4.

The Directive is based on Article 95 of the Treaty establishing the European Community (replaced by Article 114 of the Treaty on the Functioning of the European Union) concerning the establishment and functioning of the internal market. Subsequent to the adoption of the Directive, its legal basis was challenged before the European Court of Justice, on the basis that the principal objective was the investigation, detection and prosecution of serious crime. The Court held that the Directive regulated operations which were independent of the implementation of any police and judicial cooperation in criminal matters and that it harmonised neither access to data by competent national authorities nor the use and exchange of those data between those authorities. It therefore concluded that the Directive was directed essentially at the activities of operators in the relevant sector of the internal market. It accordingly upheld the legal basis[12].

---

10 Article 11 of the Directive states: 'The following paragraph shall be inserted in Article 15 of Directive 2002/58/EC:"1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks to be retained for the purposes referred to in Article 1(1) of that Directive.'

11 The Article 29 Working Party questions whether 'the [data retention] directive was meant to derogate from the general obligation [to] erase traffic data upon conclusion of the electronic communication or to mandate retention of all those data providers were already empowered to store' for their own business purposes.'

12 ECJ, C-301/6 Ireland v Parliament and Council, ECR [2009] I-00593.

3.3. Data preservation

Data retention is distinct from data preservation (also known as 'quick freeze') under which operators served with a court order are obliged to retain data relating only to specific individuals suspected of criminal activity as from the date of the preservation order. Data preservation is one of the investigative tools envisaged and used by participating states under the Council of Europe Convention on Cybercrime[13]. Almost all participating states have established a point of contact, whose role is to ensure the provision of immediate assistance in cybercrime investigations or proceedings. However, not all parties to the Convention seem to have provided for data preservation, and there has not as yet been an evaluation of how effective the model has been in tackling cybercrime[14]. Recently, a type of data preservation, known as 'quick freeze plus', has been developed. This model goes beyond data preservation in that a judge may also grant access to data which have not yet been deleted by the operators. Also, there would be a very limited exemption by law from the obligation to delete, for a short period of time, certain communication data which are not normally stored, such as location data, internet connection data and dynamic IP addresses for users which have a flat-rate subscription and where there is no need to store data for billing purposes.

Advocates of data preservation consider it to be less privacy-intrusive than data retention. However, most Member States disagree that any of the variations of data preservation could adequately replace data retention, arguing that whilst data retention results in the availability of historical data, data preservation does not guarantee the ability to establish evidence trails prior to the preservation order, does not allow investigations where a target is unknown, and does not allow for evidence to be gathered on movements of, for example, victims of or witnesses to a crime[15].

4. TRANSPOSITION OF THE DATA RETENTION DIRECTIVE

Member States were required to transpose the Directive before 15 September 2007, with the option of postponing until 15 March 2009 the implementation of retention obligations relating to internet access, internet email and internet telephony.

The analysis that follows is based on the notifications of transposition received by the Commission from 25 Member States, including Belgium which has only partially transposed the Directive[16]. In Austria and Sweden draft legislation is under discussion. In those two Member States, there is no obligation to retain data, but law enforcement authorities may and do request and obtain traffic data from operators to the extent that such data is available. Following the initial notification of transposition by Czech Republic, Germany and Romania,

---

13 Article 16 Convention on Cybercrime (http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm) .

14 Source: Council of Europe.

15 This was also recognised by the German Constitutional Court in its judgment annulling the German law transposing the Directive (see Section 4.9) (Bundesverfassungsgericht, 1 BvR 256/08 of 2 March 2010, para. 208).

16 The twenty-five Member States who have notified the Commission of transposition of the Directive are Belgium, Bulgaria, Czech Republic, Denmark, Germany, Greece, Estonia, Ireland, Spain, France, Italy, Cyprus, Latvia, Lithuania, Luxembourg, Hungary, Malta, Netherlands, Poland, Portugal, Romania, Slovenia, Slovakia, Finland and United Kingdom. Belgium informed the Commission that draft legislation completing transposition is still before Parliament.

their respective constitutional courts annulled the domestic legislation transposing the Directive[17], and they are considering how to re-transpose the Directive.

This section analyses how Member States have transposed the relevant provisions of the Directive. It also examines whether Member States have chosen to reimburse operators for the costs incurred in retaining and allowing retrieval of data, for which there is no provision in the Directive, and addresses the relevance for the Directive of the judgments of the constitutional courts of Germany, Romania and the Czech Republic.

4.1. Purpose of data retention (Article 1)

The Directive obliges Member States to adopt measures to ensure that data is retained and available for the purpose of investigating, detecting and prosecuting serious crime, as defined by each Member State in its national law. However, the purposes stated for the retention and/ or access to data in domestic legislation continues to vary in the EU. Ten Member States (Bulgaria, Estonia, Ireland, Greece, Spain, Lithuania, Luxembourg, Hungary, Netherlands, Finland) have defined 'serious crime', with reference to a minimum prison sentence, to the possibility of a custodial sentence being imposed, or to a list of criminal offences defined elsewhere in national legislation. Eight Member States (Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia, Slovenia) require data to be retained not only for investigation, detection and prosecution in relation to serious crime, but also in relation to all criminal offences and for crime prevention, or on general grounds of national or state and/or public security. The legislation of four Member States (Cyprus, Malta, Portugal, United Kingdom) refers to ‘serious crime’ or ‘serious offence’ without defining it. The details are set out in Table 1.

Table 1: Purpose limitation for data retention stated in national laws	
Belgium	For the investigation and prosecution of criminal offences, the prosecution of abuse of emergency services telephone number, investigation into malicious abuse of electronic communications network or service, for the purposes of intelligence-gathering missions undertaken by the intelligence and security services[18].
Bulgaria	For 'discovering and investigating severe crimes and crimes under Article 319a-319f of the Penal Code as well as for searching persons'[19].
Czech Republic	Not transposed.
Denmark	For investigation and prosecution of criminal acts[20].
Germany	Not transposed.

[17] Decision no 1258 from 8 October 2009 of the Romanian Constitutional Court, Romanian Official Monitor No 789, 23 November 2009; judgement of the Bundesverfassungsgericht 1 BvR 256/08, of 2 March 2010; Official Gazette of 1 April 2011, Judgment of the Constitutional Court of 22 March on the provisions of section 97 paragraph 3 and 4 of Act No. 127/2005 Coll. on electronic communications and amending certain related acts as amended, and Decree No 485/2005 Coll. on the data retention and transmission to competent authorities.

[18] Article 126(1) of Law of 13 June 2005 concerning electronic communications. .

[19] Article 250a (2), Law on Electronic Communications (amended) 2010.

[20] Article 1, Data Retention Order.

Table 1: Purpose limitation for data retention stated in national laws	
Estonia	May be used if collection of the evidence by other procedural acts is precluded or especially complicated and the object of a criminal proceeding is a criminal offence [in the first degree or an intentionally committed criminal offence in second degree with a penalty of imprisonment of at least three years][21].
Ireland	For prevention of serious offences [i.e. offences punishable by imprisonment for a term of 5 years or more, or an offence in schedule to the transposing law], safeguarding of the security of the state, the saving of human life.[22]
Greece	For the purpose of detecting particularly serious crimes[23].
Spain	For the detection, investigation and prosecution of the serious crimes considered in the Criminal Code or in the special criminal laws[24].
France	For the detection, investigation, and prosecution of criminal offences, and for the sole purpose of providing judicial authorities with information needed, and for the prevention of acts of terrorism and protecting intellectual property[25].
Italy	For detecting and suppressing criminal offences[26].
Cyprus	For investigation of a serious criminal offence[27].
Latvia	To protect state and public security or to ensure the investigation of criminal offences, criminal prosecution and criminal court proceedings[28] .
Lithuania	For the investigation, detection and prosecution of serious and very serious crimes, as defined by the Lithuanian Criminal Code[29] .
Luxembourg	For the detection, investigation, and prosecution of criminal offences carrying a criminal sentence of a maximum one year or more[30].
Hungary	To enable investigating bodies, the public prosecutor, the courts and national security agencies to perform their duties, and to enable police and the National Tax and Customs Office to investigate intentional crimes carrying a prison term of two or more years[31].

21 Subsection 110(1), Code of Criminal Procedure.

22 Article 6 Communications (Retention of Data Act) 2011.

23 Such crimes are defined in Article 4 of Law 2225/1994; Article 1 of Law 3917/2011.

24 Article 1(1), Law 25/2007.

25 The acts that regulate the use of retained data, respectively, for criminal offences, for preventing acts of terrorism and for protecting intellectual property are as follows: are Article L.34-1(II), CPCE, Law no. 2006-64 of 23 January 2006 et Law no. 2009-669 of 12 June 2009.

26 Article 132(1), Data Protection Code

27 Article 4(1), Law 183(I)/2007

28 Article 71(1), Electronic Communications Law.

29 Article 65, Law X-1835

30 Article 1(1), Law of 24 July 2010

31 For the general purpose of data retention Article 159/A of the Act C/2003, as amended by the Act CLXXIV/2007; on the purpose ofpolice access Article 68, Act XXXIV/1994; on the purpose of National Tax and Customs Office access, Article 59, Act CXXII/2010.

Table 1: Purpose limitation for data retention stated in national laws	
Malta	For investigation, detection or prosecution of serious crime[32].
Netherlands	For investigation and prosecution of serious offences for which custody may be imposed[33].
Austria	Not transposed.
Poland	For prevention or detection of crimes, for prevention and detection of fiscal offences, for use by prosecutors and courts if relevant to the court proceedings pending, for the purpose of the Internal Security Agency, Foreign Intelligence Agency, Central Anti-Corruption Bureau, Military Counter-intelligence Services and Military Intelligence Services to perform their tasks[34].
Portugal	For the investigation, detection and prosecution of serious crime[35].
Romania	Not transposed.
Slovenia	For ensuring national security, constitutional regulation and the security, political and economic interests of the state … and for the purpose of national defence[36].
Slovakia	For prevention, investigation, detection and prosecution of criminal offences[37].
Finland	For investigating, detecting and prosecuting serious crimes as set out in Chapter 5a, Article 3(1) of the Coercive Measures Act[38].
Sweden	Not transposed.
United Kingdom	For the investigation, detection and prosecution of serious crime[39].

Most transposing Member States, in accordance with their legislation, allow the access and use of retained data for purposes going beyond those covered by the Directive, including preventing and combating crime generally and the risk to life and limb. Whilst this is permitted under the e-Privacy Directive, the degree of harmonisation achieved by EU legislation in this area remains limited. Differences in the purposes of data retention are likely to affect the volume and frequency of requests and in turn the costs incurred for compliance with the obligations laid down in the Directive. Furthermore, this situation may not provide sufficiently for the foreseeability which is a requirement in any legislative measure which

32 Article 20(1), Legal Notice 198/2008.
33 Article 126, Code of Criminal Procedure.
34 Article 180a, Telecommunications Law of 16 July 2004 as amended by Article 1, Act of 24 April 2009.
35 Article 1, 3(1), Law 32/2008.
36 Article 170a(1) Electronic Communications Act.
37 Article 59a (6), Electronic Communications Act.
38 Article 14a (1), Electronic Communications Act.
39 The Data Retention (EC Directive) Regulations 2009 (2009 No. 859).

restricts the right the privacy[40]. The Commission will assess the need for, and options for achieving, a greater degree of harmonisation in this area[41].

4.2. Operators required to comply with data retention (Article 1)

The Directive applies to 'the providers of publicly available electronic communications services or of public communications networks' (Article 1(1)). Two Member States (Finland, United Kingdom) do not require small operators to retain data because, they argue, the costs both to the provider and to the state of doing so would outweigh the benefits to criminal justice systems and to law enforcement. Four Member States (Latvia, Luxembourg, Netherlands, Poland) report that they have put in place alternative administrative arrangements. While large operators present in several Member States benefit from economies of scale in terms of costs, smaller operators in some Member States tend to set up joint ventures or to outsource to companies that specialise in retention and retrieval functions in order to reduce costs. Such outsourcing of technical functions in this way does not affect the obligation of providers to supervise processing operations appropriately and to ensure the required security measures are in place, which can be problematic particularly for smaller operators. The Commission will examine the issues of security of data, and the impact on small- and medium-sized enterprises, with relation to options for amending the data retention framework.

4.3. Access to data: authorities and procedures and conditions (Article 4)

Member States are required 'to ensure that [retained data] are provided only to the competent national authorities in specific cases and in accordance with national law.' It is left to Member States to define in their national law 'the procedures to be followed and the conditions to be fulfilled in order to obtain access to retained data in accordance with necessity and proportionality requirements, subject to the relevant provisions of European Union law or public international law, and in particular the European Convention on Human Rights as interpreted by the European Court of Human Rights'.

In all Member States, the national police forces and, except in common law jurisdictions (Ireland and United Kingdom), prosecutors may access retained data. Fourteen Member States list security or intelligence services or the military among the competent authorities. Six Member States list tax and/ or customs authorities, and three list border authorities. One Member State allows other public authorities to access the data if they are authorised for specific purposes under secondary legislation. Eleven Member States require judicial authorisation for each request for access to retained data. In three Member States judicial authorisation is required in most cases. Four other Member States require authorisation from a senior authority but not a judge. In two Member States, the only condition appears to be that the request is made writing.

---

[40] Judgment of the European Court of Justice of 20 May 2003 in Joined Cases C-465/00, C-138/01 and C-139/01 (Reference for a preliminary ruling from the Verfassungsgerichtshof and Oberster Gerichtshof): Rechnungshof (C-465/00) v Österreichischer Rundfunk and Others and between Christa Neukomm (C-138/01), Joseph Lauermann (C-139/01) and Österreichischer Rundfunk (Protection of individuals with regard to the processing of personal data — Directive 95/46/EC — Protection of private life — Disclosure of data on the income of employees of bodies subject to control by the Rechnungshof).

[41] On the adoption of the Directive, the Commission issued a Declaration suggesting that the list of crimes in European Arrest Warrant should be considered. (Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States.)

Table 2: Access to retained telecommunications data		
	Competent national authorities	*Procedures and conditions*
Belgium	Judicial coordination unit, examining magistrates, public prosecutor, criminal police.	Access must be authorised by a magistrate or prosecutor. Upon request, operators must provide in 'real time' subscriber data and traffic and location data for calls made within the last month. Data for older calls must be provided as soon as possible.
Bulgaria[42]	Specific directorates and departments of the State Agency for National Security, the Ministry of the Interior, Military Information Service, Military Police Service, Minister of Defence, National Investigation Agency; the court and pre-trial authorities under the conditions.	Access only possible on the order of the Chairperson of a Regional Court.
Czech Republic	Not transposed.	
Denmark[43]	Police.	Access requires judicial authorisation; court orders are granted if application meets strict criteria on suspicion, necessity and proportionality.
Germany	Not transposed	
Estonia[44]	Police and Border Guard Board, Security Police Board and, for objects and electronic communication, the Tax and Customs Board.	Access requires permission of a preliminary investigation judge Operators must 'provide [retained data] in urgent cases not later than 10 hours and in other cases within 10 working days [of receiving a request].'
Ireland[45]	Members of Garda Síochána (police) at Chief Superintendant rank or higher; Officers of Permanent Defence Force at colonel rank or higher; Officers of Revenue Commissioners at principal officer or higher.	Requests to be in writing.
Greece[46]	Judicial, military or police public authority.	Access requires judicial decision declaring that investigation by other means is impossible or extremely difficult.
Spain[47]	Police forces responsible for detection, investigation and prosecution of the serious crimes, National Intelligence Centre and Customs Agency.	Access to these data by the competent national authorities requires prior judicial authorisation.
France[48]	Public prosecutor, designated police officers and gendarmes.	Police must provide justification for each request for access to retained data and must seek authorisation from person in the Ministry of the Interior designated by the Commission nationale de contrôle des interceptions de sécurité. Requests for access are handled by a

42 Article 250b (1), Law on Electronic Communications (amended) 2010 (authorities); Article 250b (2), 250c (1) Law on Electronic Communications (amended) 2010 (access).

43 Chapter 71, Administration of Justice Act.

44 Subsection 112(2) and (3), Code of Criminal Procedure (on authorities and procedure); Subsection 111(9) (conditions) Electronic Communications Act.

45 Article 6, Communications (Retention of Data) Bill 2009.

46 Articles 3 and 4 of Law 2225/94

47 Articles 6-7, Law 25/2007.

Table 2: Access to retained telecommunications data		
	Competent national authorities	*Procedures and conditions*
		designated officer working for the operator.
Italy[49]	Public prosecutor; police; defence counsel for either the defendant or the person under investigation.	Access requires 'reasoned order' issued by the public prosecutor.
Cyprus[50]	The courts, public prosecutor, police.	Access must be approved by a prosecutor if he considers it may provide evidence of committing a serious crime. A judge may issue such an order if there is a reasonable suspicion of a serious criminal offence and if the data are likely to be associated with it.
Latvia[51]	Authorised officers in pre-trial investigation institutions; persons performing investigative work; authorised officers in state security institutions; the Office of the Public Prosecutor; the courts.	Authorised officers, public prosecutor's office and courts are required to assess 'adequacy and relevance' of request, to record the request and ensure protection of data obtained. Authorised bodies may sign agreement with an operator e.g. for encryption of data provided.
Lithuania[52]	Pre-trial investigation bodies, the prosecutor, the court (judges) and intelligence officers.	Authorised public authorities must request retained data in writing. For access for pre-trial investigations a judicial warrant is necessary.
Luxembourg[53]	Judicial authorities (investigating magistrates, prosecutor), authorities responsible for safeguarding state security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.	Access requires judicial authorisation.
Hungary[54]	Police, National Tax and Customs Office, national security services, public prosecutor, courts.	Police and the National Tax and Customs Office require prosecutor's authorisation. Prosecutor and national security agencies may access such data without a court order.
Malta[55]	Malta Police Force; Security Service	Requests must be in writing.
Netherlands[56]	Investigating police officer	Access must be by order of a prosecutor or an investigating judge
Austria	Not transposed	
Poland[57]	Police, border guards, tax inspectors, Internal Security Agency, Foreign Intelligence Agency, Central Anti-Corruption Bureau, military counter-intelligence services, military intelligence services, the courts and the public prosecutor	Requests must be in writing and in case of police, border guards, tax inspectors, authorised by the senior official in the organisation.

48 Articles 60-1 and 60-2, Criminal Procedure Code (authorities); Article L.31-1-1 (conditions).

49 Article 132(3), Data Protection Code.

50 Article 4(2) and Article 4(4) Law 183(I)/2007.

51 Article 71(1), Electronic Communications Law (authorities); Cabinet Regulation No. 820 (procedures).

52 Article 77(1),(2) Law X-1835; oral report to the Commission.

53 Article 5-2(1) and 9(2), Law of 24 July 2010 (authorities); Article 67-1, Code of Criminal Instruction (conditions).

54 Article 68(1) and 69(1)(c)(d), Act XXXIV 1994; Articles 9/A(1) of Act V 1972; Article 71(1), (3), (4), 178/A (4), 200, 201, 268(2) Act XIX 1998; Articles 40(1), 40(2), 53(1), 54(1)(j) Act CXXV 1995.

55 Article 20(1), 20 (3) Legal Notice 198/2008.

56 Article 126ni, Code of Criminal Procedure.

57 Article 179(3), Telecommunications Law of 16 July 2004 as amended by Article 1, Act of 24 April 2009.

Table 2: Access to retained telecommunications data		
	Competent national authorities	*Procedures and conditions*
Portugal[58]	Criminal Police, National Republican Guard, Public Security Office, Military Criminal Police, Immigration and Borders Service, Maritime Police.	Transmission of data requires judicial authorisation on grounds that access is crucial to uncover the truth or that evidence would be, in any other manner, impossible or very difficult to obtain. The judicial authorisation is subject to necessity and proportional requirements.
Romania	Not transposed	
Slovenia[59]	Police, intelligence and security agencies, defence agencies responsible for intelligence and counter-intelligence and security missions.	Access requires judicial authorisation.
Slovakia[60]	Law enforcement authorities, courts.	Requests must be in writing.
Finland[61]	Police, border guards, customs authorities (for retained subscriber, traffic and location data). Emergency Response Centre, Marine Rescue Operation, Marine Rescue Sub-Centre (for identification and location data in emergencies)	Subscriber data may be accessed by all competent authorities without judicial authorisation Other data requires a court order.
Sweden	Not transposed	
United Kingdom[62]	Police, intelligence services, tax and customs authorities, other public authorities designated in secondary legislation.	Access permitted, subject to authorisation by a 'designated person' and necessity and proportionality test, in specific cases and in circumstances in which disclosure of the data is permitted or required by law. Specific procedures have been agreed with operators.

The Commission will assess the need for, and options for achieving, a greater degree of harmonisation with respect to the authorities having and the procedure for obtaining access to retained data. Options might include more clearly defined lists of competent authorities, independent and/or judicial oversight of requests for data and a minimum standard of procedures for operators to allow access to competent authorities.

4.4. Scope of data retention and categories of data covered (Articles 1(2), 3(2) and 5)

The Directive applies to the fields of fixed network telephony, mobile telephony, internet access, internet email and internet telephony. It specifies (in Article 5) the categories of data to be retained, namely data necessary for identifying:

(a) the source of a communication;

(b) the destination of a communication;

---

58 Articles 2 (1), 3(2) and 9, Law 32/2008.

59 Article 107c, Electronic Communications Act; Article. 149b, Code of Criminal Procedure; Article 24(b) Intel and Security Agency Act; Article 32, Defence Act.

60 Article 59a (8), Electronic Communications Act.

61 Article 35 (1), 36 Electronic Communications Act; Article 31-33 Police Act; Article 41, Border Guard Act.

62 Article 25, Schedule 1, Regulation of Investigatory Powers Act 2000; Article 7 Data Retention Regulation. Article 22(2) of RIPA sets down the purposes for which these authorities may acquire data.

(c) the data, time and duration of a communication;

(d) the type of a communication;

(e) users' communication equipment or what purports to be their equipment; and

(f) the location of mobile communication equipment.

It also covers (Article 3(2)) unsuccessful call attempts, that is, a communication where a telephone call has been successfully connected but not answered or where there has been a network management intervention, and where data on these attempts are generated or processed and stored or logged by operators. No data revealing the content of the communication may be retained under the Directive. It has also been subsequently clarified that search queries, that is server logs generated through the offering of a search engine service, are also outside scope of the Directive, because they are considered as content rather than traffic data[63].

Twenty-one Member States provide for the retention of each of these categories of data in their transposing legislation. Belgium has not provided for the types of telephony data to be retained, nor does it have any provision for internet-related data. Respondents to the Commission's questionnaire did not consider it necessary to amend the categories of data to be retained, although the European Parliament has issued to the Commission a Written Declaration calling for the Directive to be extended to search engines 'in order to tackle online child pornography and sex offending rapidly'[64]. In its report on the second enforcement action, the Article 29 Data Protection Working Party, argued that the categories laid down in the Directive should be considered as exhaustive, with no additional data retention obligations imposed on operators. The Commission will assess the necessity of all of these data categories.

4.5. Periods of retention (Article 6 and Article 12)

Member States are required to ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years. The maximum retention period may be extended by a Member State which is 'facing particular circumstances that warrant an extension for a limited period'; such an extension must be notified to the Commission who may decide within six months of that notification whether to approve or reject the extension. Whereas the maximum retention period may be extended, there is no provision for shortening the retention below six months. All Member States except one which have transposed the Directive apply a retention period or periods within these bounds, and there have been no notifications to the Commission of any extensions. However, there is no consistent approach across the EU.

Fifteen Member States specify a single period for all categories of data: one Member State (Poland) specifies a two-year retention period, one specifies 1.5 years (Latvia), ten specify one year (Bulgaria, Denmark, Estonia, Greece, Spain, France, Netherlands, Portugal, Finland,

---

63 Article 29 Working Party Opinion on data protection issues related to search engines, 4 April 2008.

64 Written Declaration pursuant to Rule 123 of the Rules of Procedure on setting up a European early warning system (EWS) for paedophiles and sex offenders, 19.4.2010, 0029/2010.

United Kingdom) and three specify six months (Cyprus, Luxembourg, Lithuania). Five Member States have defined different retention periods for different categories of data: two Member States (Ireland, Italy) specify two years for fixed and mobile telephony data and one year for internet access, internet email and internet telephony data; one Member State (Slovenia) specifies 14 months for telephony data and eight months for internet-related data; one Member State (Slovakia) specifies one year for fixed and mobile telephony and six months for internet-related data; one Member State (Malta) specifies one year for fixed, mobile and internet telephony data, and six months for internet access and internet email. One Member State (Hungary) retains all data for one year except for data on unsuccessful call attempts which are only retained for six months. One Member State (Belgium) has not specified any data retention period for the categories of data specified in the Directive. Details are in Table 3.

Table 3: Retention periods specified in national law	
Belgium[65]	Between 1 year and 36 months for 'publically available' telephone services. No provision for internet-related data.
Bulgaria	1 year .Data which has been accessed may be retained for a further 6 months on request.
Czech Republic	Not transposed.
Denmark	1 year
Germany	Not transposed
Estonia	1 year
Ireland	2 years for fixed telephony and mobile telephony data, 1 year for internet access, internet email and internet telephony data
Greece	1 year
Spain	1 year
France	1 year
Italy	2 years for fixed telephony and mobile telephony data, 1 year for internet access, internet email and internet telephony data
Cyprus	6 months
Latvia	18 months
Lithuania	6 months
Luxembourg	6 months
Hungary	6 months for unsuccessful calls and 1 year for all other data
Malta	1 year for fixed, mobile and internet telephony data, 6 months for internet access and internet email data
Netherlands	1 year
Austria	Not transposed
Poland	2 years
Portugal	1 year
Romania	Not transposed (6 months under the earlier annulled transposing law)
Slovenia	14 months for telephony data and 8 months for internet related data
Slovakia	1 year for fixed telephony and mobile telephony data, 6 months for internet access, internet email and internet telephony data
Finland	1 year
Sweden	Not transposed
United Kingdom	1 year

[65] Article 126(2) of Law of 13 June 2005 concerning electronic communications.

Whilst this diversity of approach is permitted by the Directive, it follows that the Directive provides only limited legal certainty and foreseeability across the EU for operators operating in more than one Member State and for citizens whose communications data may be stored in different Member States. Taking into consideration the growing internationalisation of data processing and outsourcing of data storage, options for further harmonising retention periods in the EU should be considered. With a view to meeting the proportionality principle, and in the light of light of quantitative and qualitative evidence of the value of retained data in Member States, and trends in communications and technologies and in crime and terrorism, the Commission will consider applying different periods for different categories of data, for different categories of serious crimes or a combination of the two[66]. Quantitative evidence provided by so far by Member States regarding the age of retained data suggests that around ninety percent of the data are six months old or less and around seventy percent three months old or less when the (initial) request for access is made by law enforcement authorities (see Section 5.2).

4.6. Data protection and data security and supervisory authorities (Articles 7 and 9)

The Directive requires Member States to ensure that operators respect, as a minimum, four data security principles, namely, that the retained data shall be:

(a) of the same quality and subject to the same security and protection as those data on the [public communications] network;

(b) subject to appropriate technical and organisation measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;

(c) subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only; and

(d) destroyed at the end of the period of retention, except those that have been accessed and preserved [for the purpose set down in the Directive].

In line with the Data Protection Directive and the e-Privacy Directive, operators are prohibited from processing data retained under the Directive for other purposes, provided the data would not otherwise have been retained[67]. Member States are required to designate a public authority to be responsible for monitoring, with complete independence, the application of these principles, which may be the same authorities as those required under the Data Protection Directive[68].

Fifteen Member States have transposed all of these principles in the relevant legislation. Four Member States (Belgium, Estonia, Spain, Latvia) have transposed two or three of these principles but do not explicitly provide for the destruction of data at the end of the period of retention. Two Member States (Italy, Finland) provide for the destruction of data. It is not clear which specific technical and organisational security measures, such as strong

---

66 The Commission's proposal for a directive on data retention in 2005 provided for a retention period of one year for telephony data and six months for internet data.

67 Article 13(1) Directive 95/46/EC.

68 Article 28, Directive 95/46/EC.

authentication and detailed access log management[69] have been applied. Twenty-two Member States have a supervisory authority responsible for monitoring application of the principles. In most cases this is the data protection authority. Details are in Table 4.

Table 4: Data protection and data security and supervisory authorities

Member State	*Data protection and data security provisions in national law*	*Supervisory authority*
Belgium	Operators must ensure transmission of data cannot be intercepted by a third party and must comply with ETSI standards for telecommunications security and lawful interception[70]. Principle of obligatory destruction of data at the end of the period of retention does not seem to be addressed.	Institute for Postal Services and Telecommunications
Bulgaria	Transposing law includes requirement to implement the four principles[71].	Commission for Personal Data Protection monitors processing and storing of data to ensure compliance with obligations; Parliamentary Commission in the National Assembly – monitors the procedures for authorisation and access to the data
Czech Republic[72].	Not transposed.	
Denmark	Four principles are provided for. [73].	National IT and Telecom Agency monitors the obligation for providers of electronic communications networks and services to ensure that technical equipment and systems allow police access to information about telecommunications traffic.
Germany	Not transposed.	
Estonia	Transposing law provides for three of the four principles. No explicit provision for the fourth principle though any persons whose privacy has been infringed by surveillance-related activities may request the destruction of data, subject to a court judgement[74].	Technical Surveillance Authority is the responsible authority.
Ireland[75]	Transposing law includes requirement to implement the four principles.	Designated judge has power to investigate and report on whether competent national authorities comply with provisions of transposing law.

69 Strong authentication involves dual authentication mechanisms such as password plus biometrics or password plus token in order to ensure the physical presence of the person in charge of processing traffic data. Detailed access log management involves the detailed tracking of access and processing operations through retention of logs recording user identity, access time and files accessed.

70 Article. 6, Royal Decree of 9 January 2003.

71 Article 4 (1), Law on Electronic Communications (amended) 2010

72 Sections 87 (3) and 88, Act 127/2005 as amended by Act 247/2008; Section 2, Act 336/2005; Section 3(4), Act 485/2005; Section 28(1), Act 101/2000.

73 Act on Processing Personal Data; Executive Order No.714 of 26 June 2008 on Provision of Electronic Communications Networks and Servics.

74 Subsection 111(9), Electronic Communications Act; Subsection 122(2), Code of Criminal Procedure.

75 Sections 4, 11 and 12, Communications (Retention of Data) Bill 2009.

Table 4: Data protection and data security and supervisory authorities		
Member State	*Data protection and data security provisions in national law*	*Supervisory authority*
Greece[76]	Transposing law includes requirement to implement the four principles, with further requirement for operators to prepare and apply a plan for ensuring compliance under a nominated data security manager.	Personal Data Protection Authority and Privacy of Communications Authority.
Spain[77]	Data security provisions cover three of the four principles (quality and security of retained data, access by authorised persons and protection against unauthorised processing).	Data Protection Agency is the responsible authority.
France[78]	Transposing law includes requirement to implement the four principles.	National Commission for Information Technology and Freedom supervises compliance with obligations.
Italy	No explicit provisions on security of retained data, although there is a general requirement for destruction or anonymisation of traffic data and consensual processing of location data[79].	Data protection authority monitors operators' compliance with the Directive.
Cyprus[80]	Transposing law provides for each of the four principles.	Commissioner for Personal Data Protection monitors application of transposing law.
Latvia[81]	Transposing law provides for two of the principles: confidentiality of and authorised access to retained data, and destruction of data at the end of the period of retention.	The State Data Inspectorate supervises the protection of personal data in the electronic communications sector, but not access and processing of retained data.
Lithuania[82]	Transposing law provides for the four principles.	State Data Protection Inspectorate supervises the implementation of the transposing law, and is responsible for providing the European Commission with statistics.
Luxembourg[83]	Transposing law provides for the four principles.	Data protection authority
Hungary[84]	Transposing law provides for the four principles.	Parliamentary Commissioner for Data Protection and Freedom of Information
Malta[85]	Transposing law provides for the four principles.	Data Protection Commissioner
Netherlands[86]	Transposing law provides for the four principles.	Radio Communications Agency supervises obligations of internet access and telecom providers; data protection authority supervises general processing of personal data; a protocol details their cooperation between the two authorities.

76 Article 6 of Law 3917/2011.

77 Article 8, Law 25/2007, Article 38(3) General Telecommunications Law. the Law (art 9) refers to the exception to access and cancelation rights prescribed in the Organic Law 15/1999 on personal data protection (art 22 and 23).

78 Article D.98-5, CPCE; Article L-34-1(V), CPCE; Article 34, Act n° 78-17; Article 34-1, CPCE; Article 11, Law no.78-17 of 6 January 1978.

79 Article 123, 126, Data Protection Code.

80 Articles 14 and 15, Law 183(I)/2007.

81 Article 4(4) and Article 71(6-8), Electronic Communications Law.

82 Articles. 12(5), 66(8) and (9) Electronic Communications Law as amended on 14 November 2009.

83 Article 1 (5), Law of 24 July 2010.

84 Article 157 of Act C/2003, as amended by the Act CLXXIV/2007; Article 2 of Decree 226/2003; and Act LXIII/1992 on Data Protection.

85 Article 24, 25 Legal Note 198/2008; Article 40(b) Data Protection Act (Cap.440).

Table 4: Data protection and data security and supervisory authorities		
Member State	*Data protection and data security provisions in national law*	*Supervisory authority*
Austria	Not transposed.	
Poland	Transposing law provides for the four principles[87].	Data protection authority.
Portugal	Transposing law provides for the four principles[88].	Portuguese Data Protection Authority.
Romania	Not transposed.	
Slovenia[89]	Transposing law provides for the four principles.	Information Commissioner.
Slovakia[90]	Transposing law provides for the four principles.	The national regulator and pricing authority in the area of electronic communications supervises the protection of personal data.
Finland	Transposing law only explicitly provides for the requirement to destroy data at the end of the period of retention[91].	Finish Communications Regulatory Authority supervises operators' compliance with data retention regulations. Data Protection Ombudsman supervises general legality of personal data processing.
Sweden	Not transposed.	
United Kingdom	Transposing law provides for the four principles[92].	Information Commissioner supervises the retention and/or processing of communications data (and any other personal data) and appropriate controls around data protection. The Interception Commissioner (an acting or retired senior judge) oversees the acquisition of communications data under RIPA by public authorities. Investigatory Powers Tribunal investigates complaints of misuse of their data if acquired under the transposing legislation (RIPA).

Transposition of Article 7 is inconsistent. Retained data is potentially of a highly personal and sensitive nature and high standards of data protection and data security need to be applied throughout the process, for storage, retrieval and use, and consistently and visibly in order to minimise the risk of breaches of privacy and to maintain confidence of citizens. The Commission will consider options for strengthening data security and data protection standards, including introducing privacy-by-design solutions to ensure these standards are met as part of both storage and transmission. It will also bear in mind the recommendations for minimum safeguards and for technical and organisational security measures made by the Article 29 Data Protection Working Party report on the second enforcement action[93].

---

86 Article 13(5), Telecommunications Act; the long title of the cooperation protocol is *Samenwerkingsovereenkomst tussen Agentschap Telecom en het College bescherming persoonsgegevens met het oog op de wijzigingen in de Telecommunicatiewet naar aanleiding van de Wet bewaarplicht telecommunicatiegegevens*.

87 Article 180a and 180e Telecommunications Act.

88 Article 7(1), (5) and 11, Law 32/2008; Articles 53 and 54, Personal Data Protection Act.

89 Article 107a(6) and 107c, Electronic Communications Act.

90 Article 59a, Electronic Communications Act; Article S33, Act No 428/2002 on the protection of personal data.

91 Article 16 (3), Electronic Communications Act.

92 Article 6, Data Retention Regulation.

93 Article 29 Data Protection Working Party Opinion 3/2006 (WP119); Report 01/2010.

4.7. Statistics (Article 10)

Member States are required to provide the Commission with annual statistics on data retention, including:

– cases in which information was provided to the competent authorities in accordance with applicable national law;

– the time elapsed between the data on which the data were retained and the date on which the competent authority requested the transmission of the data (i.e. the age of the data); and

– the cases where requests could not be met.

In requesting statistics pursuant to this provision, the Commission asked Member States to supply details on instances of individual 'requests' for data. Nevertheless, statistics provided differed in scope and detail: some Member States in their replies distinguished between different types of communication, some indicated the age of the data at the moment of request, while others provided only annual statistics without any detailed breakdown. Nineteen Member States[94] provided statistics on the number of requests for data for 2009 and/or 2008; this included Ireland, Greece and Austria, where data is requested despite the absence of transposing legislation at the time, and Czech Republic and Germany, whose data retention legislation has been annulled. Seven Member States which have transposed the Directive did not provide statistics, although Belgium provided an estimate of the volume of annual requests for telephony data (300 000).

Reliable quantitative and qualitative data are crucial in demonstrating the necessity and value of security measures such as data retention. This was recognised in the 2006 action plan on measuring crime and criminal justice[95] which included an objective for developing methods for regular data collection in line with the Directive and to include the statistics in the Eurostat database (providing they meet quality standards). It has not been possible to meet this objective, given that most Member States only fully transposed the Directive in the last two years and used different interpretations for the source of statistics. The Commission in its future proposal for revising the data retention framework, alongside the review of the action plan on statistics, will aim to develop feasible metrics and reporting procedures which enable transparent and meaningful monitoring of data retention and which do not place undue burdens on criminal justice systems and law enforcement authorities.

4.8. Transposition in the EEA countries

Data retention legislation is in place in Iceland, Liechtenstein and Norway[96].

---

94 Czech Republic, Denmark, Germany, Estonia, Ireland, Greece, Spain, France, Cyprus, Latvia, Lithuania, Malta, Netherlands, Austria, Poland, Slovenia, Slovakia, Finland, United Kingdom,

95 Commission Communication (2006) 437, 'Developing a comprehensive and coherent EU strategy to measure crime and criminal justice: An EU Action Plan 2006 – 2010'.

96 The transposing law in Iceland is the Telecommunication Act 81/2003 (as amended in April 2005); in Liechtenstein it is the Telecommunication Act 2006. In Norway, transposing legislation was approved on 5 April 2011, and the law is currently pending Royal Assent.

4.9. Decisions of Constitutional Courts concerning transposing laws

The Romanian Constitutional Court in October 2009, the German Federal Constitutional Court in March 2010 and the Czech Constitutional Court in March 2011 annulled the laws transposing the Directive into their respective jurisdictions on the basis that they were unconstitutional. The Romanian Court[97] accepted that interference with fundamental rights may be permitted where it respects certain rules, and provides adequate and sufficient safeguards to protect against potential arbitrary state action. However, drawing on case law of the European Court of Human Rights[98], the Court found the transposing law to be ambiguous in its scope and purpose with insufficient safeguards, and held that a 'continuous legal obligation' to retain all traffic data for six months was incompatible with the rights to privacy and freedom of expression in Article 8 of the European Convention on Human Rights.

The German Constitutional Court[99] said that data retention generated a perception of surveillance which could impair the free exercise of fundamental rights. It explicitly acknowledged that data retention for strictly limited uses along with sufficiently high security of data would not necessarily violate the German Basic Law. However, the Court stressed that the retention of such data constituted a serious restriction of the right to privacy and therefore should only be admissible under particularly limited circumstances, and that a retention period of six months was at the upper limit (*'an der Obergrenze')* of what could be considered proportionate (paragraph 215). Data should only be requested where there was already a suspicion of serious criminal offence or evidence of a danger to public security, and data retrieval should be prohibited for certain privileged communications (i.e. those connected with emotional or social need) which rely on confidentiality. Data should also be encoded with transparent supervision of their use.

The Czech Constitutional Court[100] annulled the transposing legislation on the basis that, as a measure which interfered with fundamental rights, the transposing legislation was insufficiently precise and clear in its formulation. The Court criticised the purpose limitation as insufficiently narrow given the scale and scope of the data retention requirement. It held that the definition authorities competent to access and use retained data and the procedures for such access and use were not sufficiently clear in the transposing legislation to ensure integrity and confidentiality of the data. The individual citizen, therefore, had insufficient guarantees and safeguards against possible abuses of power by public authorities. It did not criticise the Directive itself and stated that it had allowed sufficient room for the Czech Republic to transpose in accordance with the constitution. However, the Court in an *obiter dictum* did express doubt as to the necessity, efficiency and appropriateness of the retention of traffic data given the emergence of new methods of criminality such as through the use of anonymous SIM cards.

These three Member States are now considering how to re-transpose the Directive. Cases on data retention have also been brought before the constitutional courts of Bulgaria, which resulted in a revision of the transposing law, of Cyprus, in which court orders issued under the

---

97 Decision no 1258 from 8 October 2009 of the Romanian Constitutional Court,.

98 ECtHR, Rotaru v. Romania 2000, Sunday Times v. UK 1979 and Prince Hans-Adam of Liechtenstein v. Romania 2001.

99 Bundesverfassungsgericht, 1 BvR 256/08, para 1 – 345.

100 Judgment of the Czech Constitutional Court of 22 March on Act No. 127/2005 and Decree No 485/2005; see in particular paragraphs 45-48, 50-51 and 56..

transposing law were held to be unconstitutional, and of Hungary, where a case concerning the omission in the transposing law of the legal purposes of data processing is pending[101].

The Commission will consider the issues raised by national case law in its future proposal on revising the data retention framework.

4.10. Ongoing enforcement of the Directive

The Commission expects Member States who have not yet fully transposed the Directive, or who have not yet adopted legislation replacing transposing legislation annulled by national courts, to do so as soon as possible. Should this not be case, the Commission reserves its right exercise its powers under the EU Treaties. Currently, two Member States which have not transposed the Directive (Austria and Sweden) were found by the Court of Justice to have violated their obligations under EU law[102]. In April 2011 the Commission decided to refer Sweden for a second time to the Court for failure to comply with the judgment in Case C-185/09, requesting the imposition of financial penalties under Article 260 of the Treaty on the Functioning of the European Union, following a decision of the Swedish Parliament to postpone adoption of transposing legislation for 12 months. The Commission continues to monitor closely the situation in Austria which has provided a timetable for the imminent adoption of transposing legislation.

5. THE ROLE OF RETAINED DATA IN CRIMINAL JUSTICE AND LAW ENFORCEMENT

This section summarises the functions of retained data as described by Member States in their contributions to the evaluation.

5.1. Volume of retained data accessed by competent national authorities

The volume of both telecommunications traffic and requests for access to traffic data is increasing. Statistics provided by 19 Member States for either 2008 and/or 2009 indicate that, overall in the EU, over 2 million data requests were submitted each year, with significant variance between Member States, from less than 100 per year (Cyprus) to over 1 million (Poland). According to information on type of data requested which was provided by twelve Member States for either 2008 or 2009, the most frequently requested type of data was related to mobile telephony (see Tables 5, 8 and 12). Statistics do not indicate the precise purpose for which each request was submitted. Czech Republic, Latvia and Poland stated that in the case of mobile telephony data, competent authorities had to submit the same request to each of the main mobile telephone operators, and that therefore the actual numbers of requests per case were considerably lower than the statistics suggested.

There is no obvious explanation for these variances, though size of population, prevailing crime trends, purpose limitations and conditions for access and costs of acquiring data are all relevant factors.

---

[101] Bulgarian Supreme Administrative Court, decision no. 13627, 11 December 2008; Supreme Court of Cyprus Appeal Case Nos. 65/2009, 78/2009, 82/2009 and 15/2010-22/2010, 1 February 2011; the Hungarian constitutional complaint was filed by the Hungarian Civil Liberties Union on 2 June 2008.

[102] Case C-189/09 and Case C-185/09, respectively.

5.2. Age of retained data accessed

On the basis of statistical breakdown provided by nine Member States[103] for 2008 (see summary in Table 5 and further details in Annex), around ninety percent of the data accessed by competent authorities that year were six months old or less and around seventy percent three months old or less when the (initial) request for access was made.

Table 5: Overview of age of retained data accessed in nine Member States who provided breakdown by type of data in 2008

Age	*Fixed telephony*	*Mobile telephony*	*Internet data*	*Aggregate*
Under 3 months old	61%	70%	56%	67%
3-6 months old	28%	18%	19%	19%
6 to 12 months old	8%	11%	18%	12%
Over 1 year old	3%	1%	7%	2%

According to most Member States, the use of retained data older than three and even six months is less frequent but can be crucial; its use has tended to fall into three categories. Firstly, internet-related data tend to be requested later than other forms of evidence in the course of criminal investigations. Analysis of fixed network and mobile telephony data often generates potential leads which result in further requests for older data. For example, if during an investigation a name has been found on the basis of fixed network or mobile telephony data, investigators may want to identify the Internet Protocol (IP) address this person has been using and may want to identify with whom that person has been in contact over a given period of time using this IP address. In such a scenario, investigators are likely to request data allowing the tracing also of communications with other IP addresses and the identity of the persons who have used those IP addresses.

Secondly, investigations of particularly serious crimes, a series of crimes, organised crime and terrorist incidents tend to rely on older retained data reflecting the length of time taken to plan these offences, to identify patterns of criminal behaviour and relations between accomplices to a crime and to establish criminal intent. Activities connected with complex financial crimes are often only detected after several months. Thirdly, and exceptionally, Member States have requested traffic data held in another Member State, which can usually only release these data with judicial authorisation in response to a letter rogatory issued by a judge in the requesting Member State. This type of mutual legal assistance can be a lengthy process, which explains why some of the requested data was in these cases over six months old.

5.3. Cross-border requests for retained data

Criminal investigations and prosecutions may involve evidence or witnesses from, or events which took place in, more than one Member State. According to statistics provided by Member States, less than 1% of all requests for retained data concerned data held in another Member State. Law enforcement authorities indicated that they prefer to request data from domestic operators, who may have stored the relevant data, rather than launching mutual legal assistance procedure which may be time consuming without any guarantee that access to data

[103] Czech Republic, Denmark, Estonia, Ireland, Spain, Cyprus, Latvia, Malta, United Kingdom.

will be granted. Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between Member States law enforcement authorities[104], which sets deadlines for the provision of information following a request from another Member State, is not applicable because retained data is considered to be information obtained by coercive means, which is outside the scope of the instrument. Nevertheless no Member State or law enforcement authority called for such cross-border exchange to be further facilitated.

5.4. Value of retained data in criminal investigations and prosecutions

Whilst the absolute number of data requests report do not necessarily reflect the value of the data in individual criminal investigations, Member States generally reported data retention to be at least valuable, and in some cases indispensable[105], for preventing and combating crime, including the protection of victims and the acquittal of the innocent in criminal proceedings. Successful convictions rely on guilty pleas, witness statements or forensic evidence. Retained traffic data, it was reported, have proven necessary in contacting witnesses to an incident who would not otherwise have been identified, and in providing evidence of, or leads in establishing, complicity in a crime. Certain Member States[106] further claimed that the use of retained data helped to clear persons suspected of crimes without having to resort to other methods of surveillance, such as interception and house searches, which could be considered more intrusive.

There is no general definition of 'serious crime' in the EU, and there are accordingly no EU-statistics on the incidence of serious crime or of investigations or prosecutions of serious crime, though data on crime and justice are regularly published. The aggregate volume of requests for retained data as reported by the 19 Member States who supplied some sort of data for 2009 and/or 2008 was about 2.6 million. Against the latest crime and criminal justice statistics available for these 19 Member States - which refer to all crimes reported, not only serious crimes - it can be said that there were just over two requests for every police officer per year, or about 11 requests for every 100 recorded crimes[107].

On the basis of the statistics and illustrative examples provided, which link the use of retained historical communications data to the number of convictions, acquittals, cases discontinued and crimes prevented, a number of conclusions can be drawn as to the role and value of retained data for criminal investigation.

Constructing evidence trails

---

104 Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union OJ L 386 of 29/12/2006. Pp89-100 and OJ L 200 of 01/08/2007. Pp 637-648.

105 Czech Republic considered data retention 'completely indispensable in a large number of cases'; Hungary said it was 'indispensable in [law enforcement agencies'] regular activities'; Slovenia stated that the absence of retained data would 'paralyze the law enforcement agencies' operation'; a United Kingdom police agency described the availability of traffic data as 'absolutely crucial…to investigating the threat of terrorism and serious crime.'

106 Germany, Poland, Slovenia, United Kingdom.

107 In 2007 there were 1.7m police officers in EU-27, of which 1.2m were in the 19 Member States who provided statistics on requests for retained data; in 2007 there were 29.2m crimes recorded by the police in the EU, of which 24m were recorded in the 19 Member States who provided statistics. (Source: Eurostat 2009.)

Firstly, retained data enables the construction of trails of evidence leading up to an offence. They are used to discern, or to corroborate other forms of evidence on, the activities and links between suspects. Location data in particular has been used, both by law enforcement and defendants, to exclude suspects from crime scenes and to verify alibis. This evidence can therefore remove persons from criminal investigations, thus eliminating the need for more intrusive inquiries, or lead to acquittals at trial. Belgium cited the 2008 conviction of the perpetrators of the tiger kidnapping of an employee of Antwerp criminal court, in which location data linking their activities in three separate towns was decisive in convincing the jury of their complicity. In another case, that of a motorcycle-gang related murder in 2007, location data from the offenders' mobile phones proved that they were in the area when the murder took place and led to a partial confession[108]. According to Belgium, Ireland and the United Kingdom, certain crimes involving communication over the internet can *only* be investigated via data retention: for instance, threats of violence expressed in chat rooms often leave no trace other than the traffic data in cyberspace. A similar situation applies in the case of crimes carried out over the telephone. Hungary and Poland cited a case of fraud against elderly persons in late 2009/early 2010 carried out by means of telephone calls in which the perpetrators pretended to be family members in need of loans and who could only be identified through retained telephony data.

Starting criminal investigations

Secondly, there have been cases for which, in the absence of forensic or eye witness evidence, the only way to start a criminal investigation was to consult retained data. Germany cited the example of the murder of a police officer, where the assailant had escaped in the victim's vehicle, which he then abandoned. It was possible to establish that he had then telephoned for an alternative means of transport. There was no forensics or eye-witness evidence as to the identity of the murderer, and the authorities were reliant on the availability of this traffic data to enable them to pursue the investigation. In cases of internet-related child sexual abuse, data retention has been indispensable to successful investigation. Alongside other investigative techniques retained data enable identification of consumers of child abuse content[109], and support identification and rescue of child victims. Czech Republic reported that without access to retained internet-related data it would have been impossible to begin investigations as part of 'Operation Vilma' into a network of users and disseminators of child pornography. On an EU-wide level, the effectiveness of Operation Rescue (which is facilitated by Europol) in protecting children against abuse has been hindered because the absence of transposing data retention legislation has prevented certain Member States from investigating members of an extensive international paedophile network using IP addresses, which may be up to one year old.

In the investigation of cybercrime, an IP address is often the first lead. Law enforcement, through retrieval of traffic data, can identify the subscriber behind the IP address, before determining whether a criminal investigation can be launched. It can also enable police to

---

108 National Policing Improvement Agency (United Kingdom), *The Journal of Homicide and Major Incident Investigation*, Volume 5, Issue 1, Spring 2009, p. 39-51.

109 The 'Measurement and analysis of p2p activity against paedophile content' project, supported under the Safer Internet programme, provided accurate information on paedophile activity in the eDonkey peer-to-peer system, enabling identification of 178 000 users (out of 89 million users screened) who requested paedophile content.

forewarn potential victims of cyber attacks: where police manage to seize a command-and-control server used by Botnet operators, they can only see the IP addresses linked to that server; but through accessing retained data police can identify and warn potential victims owning those IP addresses.

Retained data is an integral part of criminal investigation

Thirdly, whilst law enforcement authorities and courts in most Member States do not keep statistics on what type of evidence proved crucial in securing convictions or acquittals, retained data is integral to criminal investigation and prosecution in the EU. Certain Member States said that they could not always isolate the impact of retained data on the success of criminal investigations and prosecutions, because courts consider all evidence presented to it and rarely find that a single piece of evidence was conclusive[110]. The Netherlands reported that, from January to July 2010, historical traffic data was a decisive factor in 24 court judgments. Finland reported that in 56% of the 3405 requests, retained data proved to be either 'important' or 'essential' to the detection and/or prosecution of criminal cases. The United Kingdom supplied data that sought to quantify the impact of data retention on criminal prosecutions; it reported that, for three of its law enforcement agencies, retained data was needed in most of if not all investigations resulting in criminal prosecution or conviction.

5.5. Technological developments and the use of prepaid SIM cards

Law enforcement needs to keep pace with technological developments which are used to commit or abet crime. Data retention is among the criminal investigation tools necessary to equip law enforcement authorities to address contemporary crime challenges in their diversity, volume and speed in a manageable and cost-efficient manner. A number of increasingly common forms of communication are outside the scope of the Directive. Virtual Private Networks (VPNs) in, for example, universities or large corporations, allow several users to access the internet via a single gateway using the same IP address. However, new technology permitting the attribution of addresses to individual VPN users is currently being introduced.

The proportion of mobile telephony users using prepaid services varies across the EU. Some Member States have claimed that anonymous prepaid SIM cards, especially where purchased in another Member State, could also be used by those involved in criminal activity as a means of avoiding identification in criminal investigation.[111] Six Member States (Denmark, Spain, Italy, Greece, Slovakia and Bulgaria) have adopted measures requiring the registration of prepaid SIM cards. These and other Member States (Poland, Cyprus, Lithuania) have argued in favour of an EU-wide measure for mandatory registration of the identify of users of prepaid services. No evidence has been provided as to the effectiveness of those national measures. Potential limitations have been highlighted, for example, in cases of identity theft or where a SIM card is purchased by a third party or a user roams with a card purchased in a third country. Overall the Commission is not convinced of the need for action in this area at an EU level at this stage.

---

110 Belgium, Czech Republic, Lithuania.

111 Council conclusions on combating the criminal misuse and anonymous use of electronic communications.

6. IMPACT OF DATA RETENTION ON OPERATORS AND CONSUMERS

6.1. Operators and consumers

In a joint statement to the Commission, five major industry associations stated that the economic impact of the Directive was 'substantial' or 'enormous' for 'smaller service providers', because the Directive leaves 'broad room for manoeuvre'[112]. Eight operators submitted widely varying estimates of the cost in terms of capital and operational expenditure of compliance with the Directive. These claims may be borne out by indications of the levels of reimbursement of operators' costs as reported by four of the Member States (see Table 6).

A study carried out before the transposition of the Directive in most Member States estimated the cost of setting up a system for retaining data for an internet service provider serving half a million customers to be around €375 240 in the first year and €9 870 in operational costs per month thereafter,[113] and the costs of setting up a data retrieval system to be €131 190, with operational costs of €28 960 per month. However, the German Constitutional Court in its judgment of 2 March 2010 found that the imposition of a duty of storage was 'not particularly excessively burdensome for the service providers affected [nor] disproportionate with regard to the financial burdens incurred by the enterprises as a result of the duty of storage'[114]. Per-unit data retention costs are inversely related to the size of the operator and the level of standardisation adopted by a Member State for interaction with operators[115].

Most operators in their reply to the Commission's questionnaire were unable to quantify the impact of the Directive on competition, retail prices for consumers or investment in new infrastructure and services.

There is no evidence of any quantifiable or substantial effect of the Directive on consumer prices for electronic communications services; there were no contributions to the 2009 public consultation from consumer representatives. A survey conducted in Germany on behalf of a civil society organisation indicated that consumers intended to change their communications behaviour and avoid using electronic communications services in some circumstances, however there is no corroboratory evidence for any change in behaviour having taken place in any the Member State concerned or in the EU generally[116].

The Commission intends to assess the impact of future changes to the Directive on industry and consumers including, possibly, through a specific Eurobarometer survey to gauge public perceptions.

6.2. Reimbursement of costs

The Directive does not regulate the reimbursement of costs incurred by operators as a result of the data retention requirement. These costs can be understood as:

---

112 http://www.gsmeurope.org/documents/Joint_Industry_Statement_on_DRD.PDF

113 Wilfried Gansterer & Michael Ilger, Data Retention – The EU Directive 2006/24/EC from a Technological Perspective, Wien: Verlag Medien und Recht, 2008

114 Bundesverfassungsgericht, 1 BvR 256/08 of 2 March 2010, para. 299.

115 http://www.etsi.org/website/technologies/lawfulinterception.aspx

116 The survey was carried out by Forsa and commissioned by AK Vorratsdatenspeicherung. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

(a) *operational expenditure*, that is operating costs or recurring expenses which are related to the operation of the business, a device, component, piece of equipment or facility; and

(b) *capital expenditure*, that is, expenditures creating future benefits, or the cost of developing or providing non-consumable parts for the product or system, which may include the cost of workers and facility expenses such as rent and utilities.

All Member States ensure some form of reimbursement if data are requested in the context of a criminal procedure in court. Two Member States reported that they reimburse both operational and capital expenditure. Six reimburse only operational expenditure. No other reimbursement scheme has been notified to the Commission. Details are in Table 6.

Table 6: Member States which reimburse costs

Member State	Operational expenditure	Capital expenditure	Annual reimbursement costs (million EUR)
Belgium	Yes	No	22 (2008)
Bulgaria	No	No	-
Czech Republic	Not transposed.[117]		
Denmark	Yes	No	-
Germany	Not transposed		
Estonia	Yes	No	-
Ireland	No	No	-
Greece	No	No	-
Spain	No	No	-
France	Yes	No	-
Italy	-	-	-
Cyprus	No	No	-
Latvia	No	No	-
Lithuania	Yes, if requested and justified.	No	-
Luxembourg	No	No	-
Hungary	No	No	-
Malta	No	No	-
Netherlands	Yes	No	-
Austria	Not transposed		
Poland	No	No	-
Portugal	No	No	-
Romania	Not transposed		
Slovenia	No	No	-
Slovakia	No	No	-
Finland	Yes	Yes	1
Sweden	Not transposed		
United Kingdom	Yes	Yes	55 (reimbursed overall for costs incurred over three years)

[117] Prior to the annulment of the Czech transposing law, Czech Republic did reimburse both operational and capital expenditure and reported €6.8 million in reimbursement costs for 2009.

It can be concluded from the above that the Directive has not fully achieved its aim of establishing a level playing field for operators in the EU. The Commission will consider options for minimising obstacles to the functioning of the internal market by ensuring that operators are consistently reimbursed for the costs they incur for complying with the data retention requirements, with particular attention to small- and medium-sized operators.

7. IMPLICATIONS OF DATA RETENTION FOR FUNDAMENTAL RIGHTS

7.1. The fundamental rights to privacy and the protection of personal data

Data retention constitutes a limitation of the right to private life and the protection of personal data which are fundamental rights in the EU[118]. Such a limitation must be, according to Article 52(1) of the Charter for Fundamental Rights, 'provided for by law and respect the essence of those rights, subject to the principle of proportionality', and justified as necessary and meeting the objectives of general interest recognised by the EU Union or the need to protect the rights and freedoms of others. In practice, this means that any limitation must[119]:

(a) be formulated in a clear and predictable manner;

(b) be necessary to achieve an objective of general interest or to protect the rights and freedoms of others;

(c) be proportionate to the desired aim; and

(d) preserve the essence of the fundamental rights concerned.

Article 8(2) of the European Convention of Human Rights also recognises that interference by a public authority with a person's right to privacy may be justified as necessary in the interest of national security, public safety or the prevention of crime.[120] Article 15(1) of the e-Privacy Directive and the recitals to the Data Retention Directive reiterate these principles underpinning the EU's approach to data retention.

Subsequent case law of the European Court of Justice and the European Court of Human Rights has developed the conditions which any limitation on the right to privacy must satisfy. These judgments are of relevance for whether the Directive should be amended, particularly in terms of the conditions for access and use of retained data.

Any limits on the right to privacy must be precise and enable foreseeability

In the case of Österreichischer Rundfunk, the European Court of Justice held that any interference in law with the right to privacy must be 'formulated with sufficient precision to

---

118 Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union (OJ C 83, 30.3.2010, p. 389) guarantees everyone's right to the "protection of personal data concerning him or her." Article 16 of the Treaty on the Functioning of the European Union (OJ C 83, 30.3.2010, p. 1) also enshrines everyone's right to the "protection of personal data concerning them."

119 See the Commission's Fundamental Rights Check-List for all legislative proposals in Commission Communication COM (2010) 573/4, 'Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union'.

120 Article 8, Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No 5), Council of Europe, 4.11.1950

enable the citizen to adjust his conduct accordingly… [so as to comply with] the requirement of foreseeability.'

Any limits on right to privacy must be necessary with minimum safeguards

In the case of Copland v. the United Kingdom, which concerned the monitoring by the state of a person's telephone calls, email correspondence and internet usage, the European Court of Human Rights held that such a restriction on the right to privacy could only be considered necessary if based on relevant domestic legislation[121]. In S. and Marper v. the United Kingdom, which concerned the retention of DNA profiles or fingerprints of any person acquitted of crime or whose proceedings are dropped prior to any conviction, the Court held that such a restriction on the right to privacy could only be justified if it answered a pressing social need, if it was proportionate to the aim pursued and if the reasons put forward by the public authority to justify it were relevant and sufficient[122]. The core principles of data protection required the retention of data to be proportionate in relation to the purpose of collection, and the period of storage to be limited.'[123] For telephone tapping, secret surveillance and covert intelligence-gathering 'it [was] essential… to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness.'

Any limits on the right to privacy must be proportionate to the general interest

The European Court of Justice similarly, in its ruling on the Schecke & Eifert case concerning the publication of all recipients of agricultural subsidies on the internet[124], found that it did not appear that the EU legislature had taken appropriate steps to strike a balance between respecting the essence of the right to privacy and the general interest (transparency) as recognised by the EU. In particular the Court found that the lawmakers had not taken into consideration other methods which would have been consistent with the objective whilst causing less interference with the right of recipients of subsidies to respect for their private life and protection of their personal data. Consequently, the Court held, the lawmakers had exceeded the limits of proportionality, as 'limitations in relation to the protection of personal data must apply only insofar as is strictly necessary.'

7.2. Criticisms of the principle of data retention

A number of civil society organisations wrote to the Commission arguing that data retention is, in principle, an unjustified and unnecessary restriction of individuals' right to privacy. They consider the non-consensual 'blanket and indiscriminate' retention of individuals' telecommunications traffic, location and subscriber data to be an unlawful restriction of fundamental rights. Following a case brought before the courts in one Member State (Ireland) by a civil rights group, the question of the legality of the Directive is expected to be referred

---

121 Copland v. the United Kingdom, European Court of Human Rights judgment, Strasbourg, 3.4.2007, p. 9

122 Marper v the United Kingdom, European Court of Human Rights judgment, Strasbourg, 4.12.2008, p. 31

123 Marper, p. 30.

124 C-92/09 Volker and Markus Schecke GbR v. Land Hessen and C-93/09 Eifert v. Land Hessen and Bundesanstalt für Landwirtschaft und Ernährung, 9.11.10.

to the European Court of Justice[125]. Also the European Data Protection Supervisor expressed doubts about the necessity of the measure.

7.3. Calls for stronger data security and data protection rules

The Article 29 Working Party's report on the second enforcement action argued that risks of breaches of confidentiality of communications and freedom of expression were inherent in the storage of any traffic data. It criticised certain aspects of national implementation, notably data logging, periods of retention, the type of data retained and data security measures. The Working Party reported cases in which details of the *content* of internet-related communications, outside the scope of the Directive, were retained, including destination IP addresses and URLs of websites, the header of emails and the list of recipients in the 'cc' bar. It therefore called for a clarification that the categories are exhaustive, and that no additional data retention obligations should be imposed on operators.

The European Data Protection Supervisor has asserted that the Directive 'has failed to harmonise national legislation' and that the use of retained data is not strictly limited to combating serious crime[126]. He has stated that an EU instrument containing rules on obligatory data retention should, in the event the necessity is demonstrated, also contain rules on law enforcement access and further use. He has called on the EU to adopt a comprehensive legislative framework which not only places obligations on operators to retain data, but also regulates how Member States use the data for law enforcement purposes, so as to create 'legal certainty for citizens'.

Data protection authorities in general have argued that data retention in itself implies a risk of potential breaches of privacy, which the Directive does not address at an EU level, instead requiring Member States to ensure national data protection rules are observed. Whilst there are no concrete examples of serious breaches of privacy, the risk of data security breaches will remain, and may grow with developments in technology and trends in forms of communications, irrespective of whether data are stored for commercial or security purposes, inside or outside the EU, unless further safeguards are put in place.

8. CONCLUSIONS AND RECOMMENDATIONS

This report has highlighted a number of benefits of and areas for improvement in the current data retention regime in the EU. The EU adopted the Directive at a time of heightened alert of imminent terrorist attacks. The impact assessment that the Commission intends to conduct provides an opportunity to assess the data retention in the EU against the tests of necessity and proportionality, with regard to and in the interests of internal security, the smooth functioning of the internal market and reinforcing respect for privacy and the fundamental right to protection of personal data. The Commission's proposal for revising the data retention framework should build on the following conclusions and recommendations.

---

125 On 5 May 2010 the Irish High Court granted Digital Rights Ireland Limited the motion for a reference to the European Court of Justice under Article 267 of the Treaty on the Functioning of the European Union.

126 Speech by Peter Hustinx at the conference 'Taking on the Data Retention Directive', 3 December 2010.

8.1. The EU should support and regulate data retention as a security measure

Most Member States take the view that EU rules on data retention remain necessary as a tool for law enforcement, the protection of victims and the criminal justice systems. The evidence, in the form of statistics and examples, provided by Member States is limited in some respects but nevertheless attests to the very important role of retained data for criminal investigation. These data provide valuable leads and evidence in the prevention and prosecution of crime and ensuring criminal justice. Their use has resulted in convictions for criminal offences which, without data retention, might never have been solved. It has also resulted in acquittals of innocent persons. Harmonised rules in this area should ensure that data retention is an effective tool in combating crime, that industry has legal certainty in a smoothly functioning internal market, and that the high levels of respect for privacy and the protection of personal data are applied consistently throughout the EU.

8.2. Transposition has been uneven

Transposing legislation is in force in 22 Member States. The considerable leeway left to Member States to adopt data retention measures under Article 15(1) of the e-Privacy Directive renders assessment of the Data Retention Directive highly problematic. There are considerable differences between transposing legislation in the areas of purpose limitation, access to data, periods of retention, data protection and data security and statistics. Three Member States have been in breach of the Directive since their transposing legislation was annulled by their respective constitutional courts. Two further Member States have yet to transpose. The Commission will continue to work with all Member States to help ensure effective implementation of the Directive. It will also continue in its role of enforcing EU law, ultimately using infringement proceedings if required.

8.3. The Directive has not fully harmonised the approach to data retention and has not created a level-playing field for operators

The Directive has ensured that data retention now takes place in most Member States. The Directive does not in itself guarantee that retained data are being stored, retrieved and used in full compliance with the right to privacy and protection of personal data. The responsibility for ensuring these rights are upheld lies with Member States. The Directive only sought partial harmonisation of approaches to data retention; therefore it is unsurprising that there is no common approach, whether in terms of specific provisions of the Directive, such as purpose limitation or retention periods, or in terms of aspects outside scope, such as cost reimbursement. However, beyond the degree of variation explicitly provided for by the Directive, differences in national application of data retention have presented considerable difficulties for operators.

8.4. Operators should be consistently reimbursed for the costs they incur

There continues to be a lack of legal certainty for industry. The obligation to retain and retrieve data represents a substantial cost to operators, especially smaller operators, and operators are affected and reimbursed to different degrees in some Member States compared with others, although there is no evidence that telecommunications sector overall has been adversely affected as a result of the Directive. The Commission will consider ways of providing consistent reimbursement for operators.

8.5. Ensuring proportionality in the end-to-end process of storage, retrieval and use

The Commission will ensure that any future data retention proposal respects the principle of proportionality and is appropriate for attaining the objective of combating serious crime and terrorism and does not go beyond what is necessary to achieve it. It will recognise that any exemptions or limitations in relation to the protection of personal data should only apply insofar as they are necessary. It will assess thoroughly the implications for the effectiveness and efficiency of the criminal justice system and of law enforcement, for privacy and for costs to public administration and operators, of more stringent regulation of storage, access to and use of traffic data. The following areas in particular should be examined in the impact assessment:

- consistency in limitation of the purpose of data retention and types of crime for which retained data may be accessed and used;
- more harmonisation of, and possibly shortening, the periods of mandatory data retention;
- ensuring independent supervision of requests for access and of the overall data retention and access regime applied in all Member States;
- limiting the authorities authorised to access the data;
- reducing the data categories to be retained;
- guidance on technical and organisational security measures for access to data including handover procedures;
- guidance on use of data including the prevention of data mining; and
- developing feasible metrics and reporting procedures to facilitate comparisons of application and evaluation of a future instrument.

The Commission will also consider whether and if so how an EU approach to data preservation might complement data retention.

With reference to the fundamental rights 'check-list' and the approach to information management in the area of freedom, security and justice[127], the Commission will consider each of these areas according to the principles of proportionality and the requirement of foreseeability. It will also ensure consistency with the ongoing review of the EU data protection framework[128].

8.6. Next steps

In the light of this evaluation, the Commission will propose a revision of the current data retention framework. It will devise a number of options in consultation with law enforcement,

---

127 See above reference to communication on implementation of the Charter of Fundamental Rights; 'Overview of information management in the area of freedom, security and justice', COM(2010)385, 20.07.2010

128 COM (2010) 609, 4.11.2010.

the judiciary, industry and consumer groups, data protection authorities and civil society organisations. It will research further public perceptions of data retention and its impact on behaviour. These findings will feed into an impact assessment of the identified policy options which will provide the basis for the Commission's proposal.

Annex: Additional statistics on the retention of traffic data

Notes for Annex:

1. Age of data means 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.

2. Internet-related data means data concerning internet access, internet e-mail and internet telephony.

3. Statistics for Czech Republic, Latvia and Poland subject to caveat (see Section 5.1).

Statistics submitted by Member States for 2008

Table 7: Requests for retained traffic data by age in 2008									
Age of data requested (months)/ Member State	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgium	None provided								
Bulgaria	None provided								
Czech Republic	102691	18440	10110	319	0	0	0	0	131560
Denmark	2669	672	185	37	23	2	7	4	3599
Germany	9363	2336	985	0	0	0	0	0	12684
Estonia	2773	733	157	827	0	0	0	0	4490
Ireland	8981	2016	936	1855	90	85	78	54	14095
Greece	No breakdown by age provided								584
Spain	22629	15868	10298	4783	0	0	0	0	53578
France	No breakdown by age provided								503437
Italy	None provided								
Cyprus	30	4	0	0	0	0	0	0	34
Latvia	10539	2739	1368	1211	597	438	0	0	16892
Lithuania	55735	23817	5251	512	0	0	0	0	85315
Luxembourg	None provided								
Hungary	None provided								
Malta	810	59	0	0	0	0	0	0	869
Netherlands	No breakdown by age provided								85000
Austria	No breakdown by age provided								3093
Poland	None provided								
Portugal	None provided								
Romania	None provided								
Slovenia	No breakdown by age provided								2821
Slovakia	None provided								
Finland	9134	1144	448	214	268				4008
Sweden	None provided								
United Kingdom	315350	88339	34665	19398	6385	2973	1536	1576	470222
Total	**533504**	**156167**	**64403**	**29156**	**7095***	**3230***	**1353***	**1366***	**1392281**

* Excluding Finland

Table 8: Requests for retained traffic data by type of data in 2008 (in brackets number of cases where requests for data could not be met – if provided)				
Type of data/ Member State	**Fixed network telephony**	**Mobile telephony**	**Internet-related**	**Total**
Belgium	None provided			
Bulgaria	None provided			
Czech Republic	4983 (131)	125040 (2276)	1537 (83)	131560 (2490)
Denmark	192 (0)	3273 (5)	134 (0)	3599 (5)
Germany	No breakdown by data type provided			12684 (931)
Estonia	4114 (1519)	376 (7)	None provided	4490 (1526)
Ireland	5317 (16)	5873 (48)	2905 (33)	14095 (97)
Greece	No breakdown by data type provided			584
Spain	4448 (0)	40013 (0)	9117 (0)	53578 (0)
France	No breakdown by data type provided			503437
Italy	None provided			
Cyprus	3 (0)	31 (5)	0 (0)	34 (5)
Latvia	1602 (90)	14238 (530)	1052 (76)	16892 (696)
Lithuania	765 (72)	84550 (5657)	None provided	85315 (5729)
Luxembourg	None provided			
Hungary	None provided			
Malta	29 (0)	748 (120)	92 (13)	869 (133)
Netherlands	No breakdown by data type provided			85000
Austria	No breakdown by data type provided			3093
Poland	None provided			
Portugal	None provided			
Romania	None provided			
Slovenia	No breakdown by data type provided			2821
Slovakia	None provided			
Finland	No breakdown by data type provided			4008
Sweden	None provided			
United Kingdom	90747 (0)	329421 (0)	50054 (0)	470222 (0)
Total				1392281

Table 9: Requests for retained *fixed network telephony* traffic data which were transmitted, by age, in 2008									
Age of data requested (months)/ Member State	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgium	None provided								
Bulgaria	None provided								
Czech Republic	3669	916	143	124	0	0	0	0	4852
Denmark	133	28	31	0	0	0	0	0	192
Germany	None provided								
Estonia	1876	161	74	484	0	0	0	0	2595
Ireland	4118	712	197	182	32	21	23	16	5301
Greece	None provided								
Spain	1948	1431	741	328	0	0	0	0	4448
France	None provided								
Italy	None provided								
Cyprus	3	0	0	0	0	0	0	0	3
Latvia	698	213	167	193	104	137	0	0	1512
Lithuania	251	442	0	0	0	0	0	0	693
Luxembourg	None provided								
Hungary	None provided								
Malta	28	1	0	0	0	0	0	0	29
Netherlands	None provided								
Austria	None provided								
Poland	None provided								
Portugal	None provided								
Romania	None provided								
Slovenia	None provided								
Slovakia	None provided								
Finland	None provided								
Sweden	None provided								
United Kingdom	54805	27052	5340	753	1135	437	1050	175	90747
Total	**67529**	**30956**	**6693**	**2064**	**1271**	**595**	**1073**	**191**	**110372**

Table 10: Requests for retained *mobile telephony* traffic data which were transmitted, by age, in 2008									
Age of data requested (months)/ Member State	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgium	None provided								
Bulgaria	None provided								
Czech Republic	98232	17013	7518	1	0	0	0	0	122764
Denmark	2433	628	143	33	20	1	7	3	3268
Germany	None provided								
Estonia	248	58	35	28	0	0	0	0	369
Ireland	4326	820	230	240	57	63	52	37	5825
Greece	None provided								
Spain	17403	12114	7444	3052	0	0	0	0	40013
France	None provided								
Italy	None provided								
Cyprus	23	3	0	0	0	0	0	0	26
Latvia	8928	2298	1085	746	394	257	0	0	13708
Lithuania	55484	23375	14	20	0	0	0	0	78893
Luxembourg	None provided								
Hungary	None provided								
Malta	575	53	0	0	0	0	0	0	628
Netherlands	None provided								
Austria	None provided								
Poland	None provided								
Portugal	None provided								
Romania	None provided								
Slovenia	None provided								
Slovakia	None provided								
Finland	None provided								
Sweden	None provided								
United Kingdom	229375	52241	26228	16040	3333	521	339	1344	329421
Total	**417027**	**108603**	**42697**	**20160**	**3804**	**842**	**398**	**1384**	**594915**

Table 11: Requests for retained *internet-related* traffic data which were transmitted, by age, in 2008									
Age of data requested (months)/ Member State	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgium	None provided								
Bulgaria	None provided								
Czech Republic	737	412	137	168	0	0	0	0	1454
Denmark	102	14	11	2	3	1	0	1	134
Germany	None provided								
Estonia	None provided								
Ireland	492	460	498	1422	0	0	0	0	2872
Greece	None provided								
Spain	3278	2323	2113	1403	0	0	0	0	9117
France	None provided								
Italy	None provided								
Cyprus	0	0	0	0	0	0	0	0	0
Latvia	424	150	75	219	74	34	0	0	976
Lithuania	None provided								
Luxembourg	None provided								
Hungary	None provided								
Malta	76	3	0	0	0	0	0	0	79
Netherlands	None provided								
Austria	None provided								
Poland	None provided								
Portugal	None provided								
Romania	None provided								
Slovenia	None provided								
Slovakia	None provided								
Finland	None provided								
Sweden	None provided								
United Kingdom	31170	9046	3097	2605	1917	2015	147	57	50054
Total	**36279**	**12408**	**5931**	**5819**	**1994**	**2050**	**147**	**58**	**64686**

Statistics submitted by Member States for 2009

Table 12: Requests for retained data by age in 2009									
Age of data requested (months)/ Member State	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgium	None provided								
Bulgaria	None provided								
Czech Republic	210975	56623	11620	1053	0	0	0	0	280271
Denmark	2980	685	179	104	54	38	12	14	4066
Germany	Not provided								
Estonia	4299	1836	1210	1065	0	0	0	0	8410
Ireland	8117	1652	805	297	168	134	69	41	11283
Greece	None provided								
Spain	29775	19346	13999	6970	0	0	0	0	70090
France	No breakdown by age provided								514813
Italy	None provided								
Cyprus	31	8	1	0	0	0	0	0	40
Latvia	20758	2414	1088	796	565	475	0	0	26096
Lithuania	30247	35456	5886	884	0	0	0	0	72473
Luxembourg	None provided								
Hungary	None provided								
Malta	3336	362	151	174	0	0	0	0	4023
Netherlands	None provided								
Austria	None provided								
Portugal	None provided								
Romania	None provided								
Poland	642327	178306	75525	52526	27098	23924	13984	34628	1048318
Slovenia	No breakdown by age provided								1918
Slovakia	No breakdown by age provided								5214
Finland	2000	1310	532	152	76	0	0	0	4070
Sweden	None provided								
United Kingdom	None provided								
Total	**954845**	**297998**	**110996**	**64021**	**27961**	**24571**	**14065**	**34683**	**2051085**

Table 13: Requests for retained data by type of data in 2009 (in brackets number of cases where requests for data could not be met – if provided)				
Type of data/ Member State	**Fixed network telephony**	**Mobile telephony**	**Internet-related**	**Total**
Belgium	None provided			
Bulgaria	None provided			
Czech Republic	13843 (934)	256074 (9141)	10354 (371)	280271 (10446)
Denmark	133 (0)	3771 (10)	162 (1)	4066 (11)
Germany	None provided			
Estonia	6422 (2279)	902 (21)	1086 (468)	8410 (2768)
Ireland	4542 (16)	5239 (20)	1502 (56)	11283 (92)
Greece	None provided			
Spain	5055 (0)	56133 (0)	8902 (0)	70090 (0)
France	No breakdown by data type provided			514813
Italy	None provided			
Cyprus	0 (0)	23 (3)	14 (0)	40 (3)
Latvia	1672 (218)	22796 (102)	1628 (240)	26096 (560)
Lithuania	1321 (0)	51573 (6237)	19579 (343)	72473 (6580)
Luxembourg	None provided			
Hungary	None provided			
Malta	156 (10)	3693 (882)	174 (10)	4023 (902)
Netherlands	None provided			
Austria	None provided			
Poland	No breakdown by data type provided			1048318
Portugal	None provided			
Romania	None provided			
Slovenia	No breakdown by data type provided			1918 (48)
Slovakia	No breakdown by data type provided			5214 (157)
Finland	No breakdown by data type provided			4070
Sweden	None provided			
United Kingdom	None provided			
Total				2051082 (1069885)

Table 14: Requests for retained *fixed network telephony* data which were transmitted, by age, in 2009									
Age of data requested (months)/ Member State	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgium	None provided								
Bulgaria	None provided								
Czech Republic	9919	2907	47	36	0	0	0	0	12909
Denmark	105	19	7	2	0	0	0	0	133
Germany	None provided								
Estonia	2254	866	599	424	0	0	0	0	4143
Ireland	3934	337	69	70	50	39	16	11	4526
Greece	None provided								
Spain	2371	1492	844	348	0	0	0	0	5055
France	None provided								
Italy	None provided								
Cyprus	0	0	0	0	0	0	0	0	0
Latvia	744	253	157	143	68	89	0	0	1454
Lithuania	469	773	73	6	0	0	0	0	1321
Luxembourg	None provided								
Hungary	None provided								
Malta	83	25	18	20	0	0	0	0	146
Netherlands	None provided								
Austria	None provided								
Poland	None provided								
Portugal	None provided								
Romania	None provided								
Slovenia	None provided								
Slovakia	None provided								
Finland	None provided								
Sweden	None provided								
United Kingdom	None provided								
Total	**19879**	**6672**	**1814**	**1049**	**118**	**128**	**16**	**11**	**29687**

Table 15: Requests for retained *mobile telephony* data which were transmitted, by age, in 2009									
Age of data requested (months)/ Member State	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgium	None provided								
Bulgaria	None provided								
Czech Republic	197620	48841	472	0	0	0	0	0	246933
Denmark	2777	639	162	98	47	19	12	7	3761
Germany	None provided								
Estonia	318	397	96	70	0	0	0	0	881
Ireland	3669	835	220	210	115	92	50	28	5219
Greece	None provided								
Spain	24065	15648	11147	5273	0	0	0	0	56133
France	None provided								
Italy	None provided								
Cyprus	17	16	0	0	0	0	0	0	23
Latvia	18832	1912	778	515	394	263	0	0	22694
Lithuania	25713	19595	28	0	0	0	0	0	45336
Luxembourg	None provided								
Hungary	None provided								
Malta	2332	246	111	122	0	0	0	0	2811
Netherlands	None provided								
Austria	None provided								
Poland	None provided								
Portugal	None provided								
Romania	None provided								
Slovenia	None provided								
Slovakia	None provided								
Finland	None provided								
Sweden	None provided								
United Kingdom	None provided								
Total	**275343**	**88119**	**13014**	**6288**	**556**	**374**	**62**	**35**	**383791**

Table 16: Requests for retained *internet-related* data which were transmitted, by age, in 2009									
Age of data requested (months)/ Member State	**0-3**	**3-6**	**6-9**	**9-12**	**12-15**	**15-18**	**18-21**	**21-24**	**Total**
Belgium	None provided								
Bulgaria	None provided								
Czech Republic	3369	4811	861	942	0	0	0	0	9983
Denmark	98	27	10	4	4	7	0	1	151
Germany	None provided								
Estonia	315	145	56	102	0	0	0	0	618
Ireland	489	455	502	0	0	0	0	0	1446
Greece	None provided								
Spain	3339	2206	2008	1349	0	0	0	0	8902
France	None provided								
Italy	None provided								
Cyprus	12	2	0	0	0	0	0	0	14
Latvia	852	198	74	90	88	86	0	0	1388
Lithuania	4060	15087	1	88	0	0	0	0	19236
Luxembourg	None provided								
Hungary	None provided								
Malta	150	14	0	0	0	0	0	0	164
Netherlands	None provided								
Austria	None provided								
Poland	None provided								
Portugal	None provided								
Romania	None provided								
Slovenia	None provided								
Slovakia	None provided								
Finland	None provided								
Sweden	None provided								
United Kingdom	None provided								
Total	**12684**	**22945**	**3512**	**2575**	**92**	**93**	**0**	**1**	**41902**