Home Office

A consultation paper
Transposition of Directive 2006/24/EC

Final phase of the transposition of Directive 2006/24/EC 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.

August 2008

CONTENTS

1. Executive summary

1.1 In March 2007 the Government undertook public consultation[1] on the initial transposition of European Directive 2006/24/EC ("the Directive") on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

1.2 The text of Directive 2006/24/EC is at Annex A.

1.3 The aim of the Directive is to ensure that certain data is retained to enable public authorities to undertake their lawful activities to investigate, detect[2] and prosecute crime and to protect the public.

1.4 Prior to the Government's consultation in March 2007, industry and law enforcement indicated that there was further work to do before presenting firm proposals for the implementation of the Directive with respect to internet access, internet telephony and internet email ("internet-related data"). Because of this the Government made a declaration in accordance with Article 15(3) of the Directive that it would postpone its application to the retention of internet-related data until no later than **15th March 2009.**

1.5 This consultation paper invites views on the proposed final phase for the transposition of the Directive on the retention of internet-related data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

1.6 Comments are invited on the draft Electronic Communications Data Retention (EC Directive) Regulations 2008 ("the draft Regulations") at Annex B that will enable the full implementation of the Directive.

1.7 The draft Regulations will replace the Data Retention (EC Directive) Regulations 2007[3] and will therefore incorporate the obligation to retain communications data in relation to fixed line telephony and mobile telephony, as well as internet access, internet email and internet telephony.

1.8 You are invited to provide a response by **31 October 2008.**

- by e-mail to **commsdata@homeoffice.gsi.gov.uk** or

by post to Andrew Knight, Home Office, 5th Floor, Peel Building, 2 Marsham Street, London, SW1P 4DF.

1 A consultation paper The initial transposition of Directive 2006/24/EC 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. ISBN 978-1-84726-232-5

2 Detecting crime includes establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, the gathering of evidence for use in any legal proceedings and the apprehension of the person (or persons) by whom any crime was committed. See section 81(5) of the Regulation of Investigatory Powers Act 2000.

3 SI 2007/2199

2. Introduction

2.1. This consultation paper seeks comments and suggestions on proposals to finalise the transposition of the Directive with respect to the retention of internet-related data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

2.2. Many public communications providers retain data about communications generated or processed on their networks or by the use of their services. They use this data for a variety of business reasons, including invoicing their customers, service development, site management and prevention of fraud. We refer collectively to this type of data as communications data.

2.3. The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content, not what was said or written. It includes the manner in which, and the method by which, a person or machine communicates with another person or machine.

2.4. The Directive rightly refers to atrocities in London in making the case for adopting measures for the retention of communications data across Europe. For many years this valuable data has allowed investigators to identify suspects, examine their contacts, establish relationships between conspirators and place them in a specific location. Communications data is used in numerous other ways, including assisting investigation of suspects' interaction with victims and witnesses and even in support of a suspect's alibi.

2.5. The retention of communications data in the UK has been recognised as a valuable and important measure for a number of years – it has been our policy since 2001 under Part 11 of the Anti-Terrorism, Crime and Security Act 2001[4] (ATCSA) and has been in practice since 2003, following publication of the code of practice[5] on voluntary retention of communications data.

2.6. Many public communications providers will be unaffected by these proposals to legislate on retention of internet-related data - either because their business practices involve retaining such data for their own purposes for as long or longer than the proposed retention period or because their business practice means that the required data is retained by another public communications provider in the UK. Consultation question 1 invites comments on the application of the Directive:

Question 1: Will individual public communications providers be able to interpret how the draft Regulation would apply to their business? If not, why not?

2.7. The proposed Regulations will not prevent businesses from keeping internet-related data for longer than our proposed retention period (so long as they comply with the Data Protection Act 1998[6]). Our aim is to ensure that this data is available for a minimum of 12 months to assist in the investigation, detection and prosecution of serious crime[7].

4 Part 11 of the Anti-Terrorism, Crime and Security Act 2001 can be found at http://www.opsi.gov.uk/ACTS/acts2001/10024--l.htm#102
5 The code of practice on voluntary retention of communications data can be found at: http://www.opsi.gov.uk/si/si2003/draft/5b.pdf
6 The Data Protection Act 1998 can be found at: http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1
7 Serious crime is determined by applying a test at to whether:
(a) a person aged 21 years and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more;
(b) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

2.8. The Directive represents a transition from a voluntary regime for retention of communications data in the UK, to a framework which mandates minimum requirements for retention of internet-related data across EU Member States.

2.9. The Directive required Member States to put measures in place by 15 September 2007. However, the implementation of internet-related aspects of the Directive was postponed in the UK until 15 March 2009. We recognised that the retention of communications data relating to the internet is a more complex issue involving much larger volumes of data and a considerably broader set of stakeholders within the industry so our initial transposition of the Directive dealt only with fixed line and mobile telephony.

2.10. Our approach to transposing the Directive was developed using an Impact Assessment (IA)[8]. We have included the IA at Annex C

2.11. More information about the IA process can be found at:

http://www.berr.gov.uk/bre/policy/scrutinising-new-regulations/preparing-impact-assessments/page44077.html

2.12. This consultation provides an opportunity to tell the Government if there is anything different that should be included in the draft Regulations before they are laid before Parliament for approval later this year.

8 A partial RIA was included in our - A consultation paper The initial transposition of Directive 2006/24/EC 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. ISBN 978-1-84726-232-5

3. Human Rights considerations

3.1 A key aspect of the debate, both during the public consultation on, and parliamentary debate about, the code of practice for voluntary retention of data, and also during the debate about the Directive within the European Council and the European Parliament, has been the impact, or potential impact, that retention of communications data has on individuals' human rights. The implementation of the Directive does not alter the balance in that debate and we consider that these measures are a proportionate interference with individuals' right to privacy to ensure protection of the public. Previous debates have concluded that the retention period is a significant factor in determining proportionality. In the draft Regulations at Annex A, we propose to continue with a retention period of 12 months

4. What is communications data?

4.1. The term communications data, which is expressed in the Directive and draft Regulations as 'data', does **not** refer to the content of communications. It's about:

- Who is communicating with whom?
- When and where are they communicating?
- What type of communication is it?

4.2. In the context of the draft Regulations, 'communications data'[9] is defined as 'traffic data and location data and the related data necessary to identify the subscriber or user'. 'Traffic data and location data' have the same meaning as in the Privacy and Electronic Communications (EC Directive) Regulation 2[10]. This defines these terms as:

"location data" means any data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to -

- the latitude, longitude or altitude of the terminal equipment
- the direction of travel of the user; or
- the time the location information was recorded;

"traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication'

4.3. The data that must be retained by public communications providers is defined in Article 5 of the Directive, and is specified in regulations 5, 6 and 7 of the draft Regulations. The way in which we specify the data to be retained is the subject of consultation question 2:

Question 2: Is the data required to be retained specified clearly in the draft Regulations? If not, why not and can the specification be clearer?

9 The definition of the 'data' in these Regulations is within the scope of Section 21(4) of the Regulation of Investigatory Powers Act 2000.
10 The Privacy and Electronic Communications Regulations can be found at: http://www.opsi.gov.uk/si/si2003/20032426.htm

5. Why is it important to retain communications data?

5.1. The value of communications data and the importance of ensuring its retention has been discussed extensively, in the UK during the:

- development of Part 11 of ATCSA in 2001;
- consultation on the code of practice for the voluntary retention of communications data in 2003;
- consultation concerning the implementation of Chapter 2 of Part I of the Regulation of Investigatory Powers Act 2000 (RIPA)[11] which governs access to communications data in 2003;
- consultation in 2006 on the code of practice[12] which accompanies Chapter 2 of Part I of the RIPA and was implemented in 2007.

There has also been extensive discussion across Europe during the development of the Directive itself. This section reiterates the reasons why communications data is so valuable and why it is necessary to make legislative provisions to ensure that it is retained. Where possible, we have provided illustrative case studies.

5.2. The following description of the use of communications data was provided in the 2003 consultation paper:

'Access to such communications data allows investigators to identify suspects, examine their contacts, establish relationships between conspirators, and place them in a specific location at a certain time. Analysis of this information can then be used to draw up a detailed profile of the suspect(s), either to inform prevention/disruption operations or for use as corroborative evidence in a prosecution supported by witness statements. Equally, the information provided by analysis of communications data may be used to clear an individual, or individuals, of any suspicion.'

11 Access to Communications Data – Respecting Privacy and Protecting the Public From Harm, published by Home Office, Communications Directorate, Ref 000427 March 2003

12 ISBN 1-84473-915-5

The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children. The internet is integral to the lives of children of all ages. It opens up new opportunities and is now an essential part of their every day world whether they are using it for homework, to talk and share materials with their friends or for a multitude of other uses that are legitimate and beneficial in so many ways.

But where children go then child sex offenders will follow – whether in the real or virtual world.

The vast majority of CEOP's work is by resolution of IP addresses, e-mail addresses and increasingly mobile phone numbers. During the period March to June 2008 CEOP identified 96 suspects (who have been arrested) and safeguarded 30 children through the use of internet related data, for example:

- On the 2nd November 2007 CEOP received intelligence from the FBI that an individual using internet e-mail had sent a movie file of a woman sexually abusing a 4 month old baby girl. The log-on IP address for this account was assigned to a UK service provider and found to be registered to a male resident in Northampton. Enquiries established this individual had a girlfriend who had three children all less than 4 years of age. Investigations commenced and both were later convicted of the serious sexual abuse of the children. The children were found in conditions of neglect, described by an officer as *utterly filthy, unsanitary and unfit for human residence.*
- During a proactive operation, CEOP identified a person who was distributing child abuse images on-line. The IP address was identified and consequential subscriber information identified a suspect. The police later arrested the suspect and seized and examined his computer equipment and a large quantity of serious sexually explicit (level 4 & 5 SAP) images retrieved. The suspect also had his DNA taken (he was not previously known to police), which was then compared to samples on the DNA database. That comparison linked him directly to a sexual assault on 3 yr old child in restaurant toilet, an offence for which he has been convicted.

5.3. Often such communications data is needed very soon after the communication has taken place – for example, sexual offenders grooming children for sexual purposes within the online environment or where a hostage has been taken and ransom demands made. In such circumstances, it is likely that the public communications provider will still have the data – although it might be difficult to access.

5.4. Increasingly, public communications providers are retaining communications data for shorter periods. Partly this is because business practices are evolving and the data is less relevant to the public communications providers and partly this is because the Data Protection Act has encouraged the industry to delete data more efficiently once the business purpose for retaining it has expired.

The West Yorkshire Police provided the following examples where internet related data had assisted their officers to identify and arrest a team of armed robbers, identify someone engaged in self harm and determine a bomb threat was in fact a hoax:

- Operation Backfill was an investigation into a serious of armed robberies where high value Audi motor cars were advertised for sale for "strictly cash only". The advertisements were posted on a website which specialised in the sale of used cars. When potential customers met up with the persons purporting to sell the cars they were held at gun point and demands made for their monies. The police commenced an investigation which examined the criminal's use of the internet. The investigators acquired internet related data (MAC address and consequential subscriber information) from the service provider which indicated the use of a lap top computer and premises from where the suspects had logged onto the internet when posting the advertisements. The suspects were arrested;
- Two people were engaged in an 'internet chat session', one in the United States and the second in Bradford. During the session the man in Bradford stated he had deliberately stabbed himself and was likely to bleed to death. The police were alerted and the acquisition of internet related data (IP address and consequential subscriber information) indicated the house where the man was. The police were able to intervene and assist the injured man;
- A series of internet e-mails were sent to a confidential help-line run by a charity threatening to "bomb" their office premises. The investigation determined, through the acquisition and analysis of internet related data, that the bomb threats were a hoax.

5.5. A two week survey of communications data obtained by the police in the UK was conducted by the Association of Chief Police Officers (ACPO) Data Communications Group in May 2005. During the survey, there were 231 requests for data relating to communications that had taken place between 6 and 12 months earlier. 60% of these requests were in support of murder and terrorism investigations and 26% of the requests were in support of other forms of serious crime including armed robbery and firearms offences.

The Greater Manchester Police provided the following examples where internet related data had assisted their officers to save life, determine whether or not a crime has been committed and seek the whereabouts of a suspect:

- A woman intending to take her own life was communicating her intention by means of internet e-mail to a person chosen at random. Urgent liaison with the service provider determined the woman's subscriber details relating to her e-mail address and assisted the police to locate her and intervene;
- The police officers investigated an allegation of kidnap concerning two women being held hostage in the Salford area of Greater Manchester. The alert of the kidnap was apparently communicated by one of the women by use of her internet e-mail. Urgent liaison by the police with the service provider established the internet e-mail account had been logged on from a location in Slovenia. Police officers visited the women's home addresses and established the allegation was malicious and the women were safe and well;
- A man, wanted in connection with the rape of a young child, fled the country to evade capture. The police became aware he was still sending and receiving internet e-mails from his account and undertook the acquisition of internet related data (IP addresses and associated subscriber data) which indicated the location from where he was logging onto his internet e-mail account and established he was initially in Spain and then France. The data assisted the police to focus their investigations with colleagues in France and international warrants were issued for his arrest.

5.6. The requirement for data older than 6 months is predominantly for long-running serious crime investigations. This highlights the significance of this older data which without a mandatory framework for retention in place is more at risk of deletion. We believe that retention of this data is justified by the benefit to national security and the prevention of serious crime.

The Serious Organised Crime Agency (SOCA) provided the following examples where internet related data had assisted their officers to identify the whereabouts of a murder suspect and reveal the identity of a blackmailer:

- A foreign citizen was wanted for murder in his home country and it was believed he had fled to another country and his whereabouts unknown. The investigation identified the suspect was using internet e-mail provided by a UK based service provider. The SOCA officers undertook the acquisition of internet related data which indicated the location from where the suspect was logging onto his internet e-mail account which led directly to his arrest;
- An offender residing in the UK was using an internet e-mail account to communicate with a company he was attempting to blackmail. The SOCA officers undertook the acquisition of internet related data (IP addresses and associated subscriber data) which indicated locations from where the offender had accessed his internet e-mail account. The analysis of the data further revealed his identity and he was arrested.

Proposal to transpose Directive 2006/24/EC

5.7. We propose to complete the implementation of the Directive using the draft Regulations at Annex B. The draft Regulations also revoke the Data Retention (EC Directive) Regulations 2007 which are superseded by these Regulations. Following public consultation, we intend to lay a revised draft of these Regulations before Parliament later this year under the European Communities Act of 1972. The draft Regulations are subject to the affirmative resolution procedure and will require the approval of both Houses of Parliament.

5.8. Whilst there are no provisions within the Directive to reimburse public communications providers for additional costs incurred in meeting the requirements of the Directive, the European Commission made a declaration to the European Council on this subject in February 2006:

'The Commission recognises that retention of data may generate significant additional costs for electronic communication providers, and that reimbursement by Member States of demonstrated additional costs incurred by undertakings for the sole purpose of complying with requirements imposed by national measures implementing this Directive for the purposes as set out in the Directive may be necessary. In assessing the compatibility of such aids with the Treaty, the Commission will, inter alia, take due account of such necessity and of the benefits in terms of public security impact on society in general of the data retention obligations flowing from the Directive.'

5.9. In the UK, we propose to make provision for payment to public communications providers of additional expenses. These provisions can be found in draft Regulation 10 at Annex B. Section 4 of the Impact Assessment at Annex C sets out why we believe these payments are necessary and consultation questions 3 and 4 invite comments on this:

Question 3: Do you agree with the Government's approach to meet additional expenses to reduce burden and meet requirements?

Question 4: Do you agree the proposed approach will not have a detrimental effect upon competition?

5.10. Ireland and Slovakia have challenged the legal basis of the Directive before the European Court of Justice albeit neither Government is challenging the principles behind retention of communications data; indeed Ireland has in place its own domestic legislation for retention of communications data. Regulations passed by Parliament under the European Community Act 1972 will be unaffected if the Directive is subsequently annulled.

5.11. Until the transposition of the Directive is completed and provisions are in place for the retention of internet-related data, we will continue with voluntary arrangements for the retention of these types of data under Part 11 of ATCSA. In addition the voluntary code will continue to apply to communications data not covered by the Directive. This may include new forms of communications data which emerge as technology develops.

Question 5: Do you think the draft Regulations can provide a framework that will enable implementation of the internet aspects of the Directive?

6. Consultation Questions

6.1. Your comments and views are invited on the following questions:

1. Will individual public communications providers be able to interpret how the draft Regulation would apply to their business? If not, why not?
2. Is the data required to be retained specified clearly in the draft Regulations? If not, why not and can the specification be clearer?
3. Do you agree with the Government's approach to meet additional expenses to reduce burden and meet requirements?
4. Do you agree the proposed approach will not have a detrimental effect upon competition?
5. Do you think the draft Regulations can provide a framework that will enable implementation of the internet aspects of the Directive?

7. How to respond

7.1. Please send all responses to this consultation by **31 October 2008:**

- By e-mail: commsdata@homeoffice.gsi.gov.uk
- By post: Andrew Knight, Home Office, 5th Floor Peel, 2 Marsham Street, London, SW1P 4DF.

Alternative formats

7.2. Should you require a copy of this consultation paper in any other format, please contact Andrew Knight.

Responses: Confidentiality & Disclaimer

1. The information you send us may be passed to colleagues within the Home Office, the Government or related agencies.
2. It is intended to publish a summary of responses to this consultation on the Home Office web site. Information provided in response to this consultation, including personal information, may be published or disclosed in accordance with the access to information regimes (these are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 1998 (DPA) and the Environmental Information Regulations 2004).
3. If you want the information that you provide to be treated as confidential, please be aware that, under the FOIA, there is a statutory Code of Practice with which public authorities must comply and which deals, amongst other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential. If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding on the Department.
4. Please ensure that your response is marked clearly if you wish your response and name to be kept confidential.
5. Confidential responses will be included in any statistical summary of numbers of comments received and views expressed.
6. The Department will process your personal data in accordance with the DPA - in the majority of circumstances this will mean that your personal data will not be disclosed to third parties.
7. This consultation follows the Cabinet Office Code of Practice on Consultation – the criteria for which are set out in Annex E.

HOME OFFICE
August 2008

ANNEX A

DIRECTIVE 2006/24/EC
EUROPEAN UNION

THE EUROPEAN PARLIAMENT **THE COUNCIL**

Strasbourg, 15 March 2006
(OR. en)

2005/0182 (COD)
LEX 687

PE-CONS 3677/12/05
REV 12

COPEN 200
TELECOM 151
CODEC 1206

DIRECTIVE OF THE EUROPEAN PARLIAMENT
AND OF THE COUNCIL
ON THE RETENTION OF DATA GENERATED OR
PROCESSED IN CONNECTION WITH THE PROVISION
OF PUBLICLY AVAILABLE ELECTRONIC
COMMUNICATIONS SERVICES OR OF
PUBLIC COMMUNICATIONS NETWORKS AND
AMENDING DIRECTIVE 2002/58/EC

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 networksand amending Directive 2002/58/EC

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,
Having regard to the proposal from the Commission,
Having regard to the Opinion of the European Economic and Social Committee[1],
Acting in accordance with the procedure laid down in Article 251 of the Treaty[2],

1 Opinion delivered on 19 January 2006 (not yet published in the Official Journal).
2 Opinion of the European Parliament of 14 December 2005 (not yet published in the Official Journal) and Council Decision of 21 February 2006.

Whereas:

(1) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3] requires Member States to protect the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the Community.

(2) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[4] translates the principles set out in Directive 95/46/EC into specific rules for the electronic communications sector.

(3) Articles 5, 6 and 9 of Directive 2002/58/EC lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data must be erased or made anonymous when no longer needed for the purpose of the transmission of a communication, except for the data necessary for billing or interconnection payments. Subject to consent, certain data may also be processed for marketing purposes and the provision of value-added services.

(4) Article 15(1) of Directive 2002/58/EC sets out the conditions under which Member States may restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of that Directive. Any such restrictions must be necessary, appropriate and proportionate within a democratic society for specific public order purposes, i.e. to safeguard national security (i.e. State security), defence, public security or the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications systems.

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

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

3 OJ L 281, 23.11.1995, p. 31. Directive as amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).
4 OJ L 201, 31.7.2002, p. 37.

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

(8) The Declaration on Combating Terrorism adopted by the European Council on 25 March 2004 instructed the Council to examine measures for establishing rules on the retention of communications traffic data by service providers.

(9) Under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), everyone has the right to respect for his private life and his correspondence. Public authorities may interfere with the exercise of that right only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety, for the prevention of disorder or crime, or for the protection of the rights and freedoms of others. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR is therefore a necessary measure.

(10) On 13 July 2005, the Council reaffirmed in its declaration condemning the terrorist attacks on London the need to adopt common measures on the retention of telecommunications data as soon as possible.

(11) Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.

(12) Article 15(1) of Directive 2002/58/EC continues to apply to data, including data relating to unsuccessful call attempts, the retention of which is not specifically required under this Directive and which therefore fall outside the scope thereof, and to retention for purposes, including judicial purposes, other than those covered by this Directive.

(13) This Directive relates only to data generated or processed as a consequence of a communication or a communication service and does not relate to data that are the content of the information communicated. Data should be retained in such a way as to avoid their being retained more than once. Data generated or processed when supplying the communications services concerned refers to data which are accessible. In particular, as regards the retention of data relating to Internet e-mail and Internet telephony, the obligation to retain data may apply only in respect of data from the providers' or the network providers' own services.

(14) Technologies relating to electronic communications are changing rapidly and the legitimate requirements of the competent authorities may evolve. In order to obtain advice and encourage the sharing of experience of best practice in these matters, the Commission intends to establish a group composed of Member States' law enforcement authorities, associations of the electronic communications industry, representatives of the European Parliament and data protection authorities, including the European Data Protection Supervisor.

(15) Directive 95/46/EC and Directive 2002/58/EC are fully applicable to the data retained in accordance with this Directive. Article 30(1)(c) of Directive 95/46/EC requires the consultation of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established under Article 29 of that Directive.

(16) The obligations incumbent on service providers concerning measures to ensure data quality, which derive from Article 6 of Directive 95/46/EC, and their obligations concerning measures to ensure confidentiality and security of processing of data, which derive from Articles 16 and 17 of that Directive, apply in full to data being retained within the meaning of this Directive.

(17) It is essential that Member States adopt legislative measures to ensure that data retained under this Directive are provided to the competent national authorities only in accordance with national legislation in full respect of the fundamental rights of the persons concerned.

(18) In this context, Article 24 of Directive 95/46/EC imposes an obligation on Member States to lay down sanctions for infringements of the provisions adopted pursuant to that Directive. Article 15(2) of Directive 2002/58/EC imposes the same requirement in relation to national provisions adopted pursuant to Directive 2002/58/EC. Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[5] provides that the intentional illegal access to information systems, including to data retained therein, is to be made punishable as a criminal offence.

(19) The right of any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with national provisions adopted pursuant to Directive 95/46/EC to receive compensation, which derives from Article 23 of that Directive, applies also in relation to the unlawful processing of any personal data pursuant to this Directive.

5 OJ L 69, 16.3.2005, p. 67.

(20) The 2001 Council of Europe Convention on Cybercrime and the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data also cover data being retained within the meaning of this Directive.

(21) Since the objectives of this Directive, namely to harmonise the obligations on providers to retain certain data and to ensure that those data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law, cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of this Directive, be better achieved at Community level, the Community may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty. In accordance with the principle of proportionality, as set out in that Article, this Directive does not go beyond what is necessary in order to achieve those objectives.

(22) This Directive respects the fundamental rights and observes the principles recognised, in particular, by the Charter of Fundamental Rights of the European Union. In particular, this Directive, together with Directive 2002/58/EC, seeks to ensure full compliance with citizens' fundamental rights to respect for private life and communications and to the protection of their personal data, as enshrined in Articles 7 and 8 of the Charter.

(23) Given that the obligations on providers of electronic communications services should be proportionate, this Directive requires that they retain only such data as are generated or processed in the process of supplying their communications services. To the extent that such data are not generated or processed by those providers, there is no obligation to retain them. This Directive is not intended to harmonise the technology for retaining data, the choice of which is a matter to be resolved at national level.

(24) In accordance with paragraph 34 of the Interinstitutional agreement on better law-making[6], Member States are encouraged to draw up, for themselves and in the interests of the Community, their own tables illustrating, as far as possible, the correlation between this Directive and the transposition measures, and to make them public.

(25) This Directive is without prejudice to the power of Member States to adopt legislative measures concerning the right of access to, and use of, data by national authorities, as designated by them. Issues of access to data retained pursuant to this Directive by national authorities for such activities as are referred to in the first indent of Article 3(2) of Directive 95/46/EC fall outside the scope of Community law. However, they may be subject to national law or action pursuant to Title VI of the Treaty on European Union. Such laws or action must fully respect fundamental rights as they result from the common constitutional traditions of the Member States and as guaranteed by the ECHR. Under Article 8 of the ECHR, as interpreted by the European Court of Human Rights, interference by public authorities with privacy rights must meet the requirements of necessity and proportionality and must therefore serve specified, explicit and legitimate purposes and be exercised in a manner that is adequate, relevant and not excessive in relation to the purpose of the interference,

6 OJ C 321, 31.12.2003, p. 1.

HAVE ADOPTED THIS DIRECTIVE:

Article 1

Subject matter and scope

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

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network.

Article 2

Definitions

1. For the purpose of this Directive, the definitions in Directive 95/46/EC, in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)[7], and in Directive 2002/58/EC shall apply.

2. For the purpose of this Directive:

   (a) "data" means traffic data and location data and the related data necessary to identify the subscriber or user;

   (b) "user" means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

   (c) "telephone service" means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

   (d) "user ID" means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service;

   (e) "cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated;

   (f) "unsuccessful call attempt" means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

7 OJ L 108, 24.4.2002, p. 33

Article 3

Obligation to retain data

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

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

Article 4

Access to data

Member States shall adopt measures to ensure that data retained in accordance with this Directive are provided only to the competent national authorities in specific cases and in accordance with national law. The procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights.

Article 5

Categories of data to be retained

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

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

(1) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

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

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID(s) allocated;

(ii) the user ID and telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

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

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

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

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

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

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

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

(1) concerning fixed network telephony and mobile telephony:

the telephone service used;

(2) concerning Internet e-mail and Internet telephony:

the Internet service used;

(e) data necessary to identify users' communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;

(v) the IMEI of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

(3) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone number for dial-up access;

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

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

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

(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

Article 6

Periods of retention

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

Article 7

Data protection and data security

Without prejudice to the provisions adopted pursuant to Directive 95/46/EC and Directive 2002/58/EC, each Member State shall ensure that providers of publicly available electronic communications services or of a public communications network respect, as a minimum, the following data security principles with respect to data retained in accordance with this Directive:

(a) the retained data shall be of the same quality and subject to the same security and protection as those data on the network;

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

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

(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention.

Article 8

Storage requirements for retained data

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

Article 9

Supervisory authority

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

2. The authorities referred to in paragraph 1 shall act with complete independence in carrying out the monitoring referred to in that paragraph.

Article 10

Statistics

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

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

   – the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data;

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

2. Such statistics shall not contain personal data.

Article 11

Amendment of Directive 2002/58/EC

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

"1a. Paragraph 1 shall not apply to data specifically required by Directive 2006/…/EC of the European Parliament and of the Council of 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.

Article 12

Future measures

1. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 may take the necessary measures. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them.

2. The Commission shall, within a period of six months after the notification referred to in paragraph 1, approve or reject the national measures concerned, after having examined whether they are a means of arbitrary discrimination or a disguised restriction of trade between Member States and whether they constitute an obstacle to the functioning of the internal market. In the absence of a decision by the Commission within that period the national measures shall be deemed to have been approved.

3. Where, pursuant to paragraph 2, the national measures of a Member State derogating from the provisions of this Directive are approved, the Commission may consider whether to propose an amendment to this Directive.

Article 13

Remedies, liability and penalties

1. Each Member State shall take the necessary measures to ensure that the national measures implementing Chapter III of Directive 95/46/EC providing for judicial remedies, liability and sanctions are fully implemented with respect to the processing of data under this Directive.

2. Each Member State shall, in particular, take the necessary measures to ensure that any intentional access to, or transfer of, data retained in accordance with this Directive that is not permitted under national law adopted pursuant to this Directive is punishable by penalties, including administrative or criminal penalties, that are effective, proportionate and dissuasive.

Article 14

Evaluation

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

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

Article 15

Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by no later than .....**. They shall forthwith inform the Commission thereof.

   When Member States adopt those measures, they shall contain a reference to this Directive or shall be accompanied by such reference on the occasion of their official publication. The methods of making such reference shall be laid down by Member States.

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

3. Until …[8], each Member State may postpone application of this Directive to the retention of communications data relating to Internet Access, Internet telephony and Internet e-mail. Any Member State that intends to make use of this paragraph shall, upon adoption of this Directive, notify the Council and the Commission to that effect by way of a declaration. The declaration shall be published in the Official Journal of the European Union.

Article 16

Entry into force

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

Article 17

Addressees

This Directive is addressed to the Member States.

Done at Strasbourg,

For the European Parliament
The President

For the Council
The President

8 36 months after the date of adoption of this Directive.

ANNEX B

Draft Regulations laid before Parliament under paragraph 2(2) of Schedule 2 to the European Communities Act 1972, for approval by resolution of each House of Parliament.

DRAFT STATUTORY INSTRUMENTS

2008 No.

ELECTRONIC COMMUNICATIONS

The Data Retention (EC Directive) Regulations 2008

Made - - - - ***

Coming into force - - *15th March 2009*

The Secretary of State, being a Minister designated([1]) for the purposes of section 2(2) of the European Communities Act 1972([2]) in respect of matters relating to electronic communications, in exercise of the powers conferred upon him by that section, makes the following Regulations (a draft of which has been approved by each House of Parliament):

Citation and commencement

1.—(1) These Regulations may be cited as the Data Retention (EC Directive) Regulations 2008.

(2) These Regulations come into force on 15th March 2009.

Interpretation

2. In these Regulations—

(a) "cell ID" means the identity or location of the cell from which a mobile telephony call was made or received;

(b) "communications data" means traffic data and location data and the related data necessary to identify the subscriber or user;

1 S.I. 2001/3495.
2 1972 c. 68.

(c) "the Data Retention Directive" means 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;

(d) "location data" means data processed in an electronic communications network indicating the geographical position of the terminal equipment of a user of a public electronic communications service, including data relating to—

(i) the latitude, longitude or altitude of the terminal equipment,

(ii) the direction of travel of the user, or

(iii) the time the location information was recorded;

(e) "public communications provider" means—

(i) a provider of a public electronic communications network, or

(ii) a provider of a public electronic communications service;

and "public electronic communications network" and "public electronic communications service" have the meaning given in section 151 of the Communications Act 2003( );

(f) "telephone service" means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

(g) "traffic data" means data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication;

(h) "user ID" means a unique identifier allocated to persons when they subscribe to or register with an internet access service or internet communications service.

Communications data to which these Regulations apply

3. These Regulations apply to communications data if, or to the extent that, the data are generated or processed in the United Kingdom by public communications providers in the process of supplying the communications services concerned.

Obligation to retain communications data

4.—(1) It is the duty of a public communications provider to retain the communications data specified in the following provisions—

(a) regulation 5 (fixed network telephony);

(b) regulation 6 (mobile telephony);

(c) regulation 7 (internet access, internet e-mail or internet telephony).

(2) The obligation extends to data relating to unsuccessful call attempts that—

(a) in the case of telephony data, are stored in the United Kingdom, or

(b) in the case of internet data, are logged in the United Kingdom.

(3) An "unsuccessful call attempt" means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention.

(4) The obligation does not extend to unconnected calls.

(5) No data revealing the content of a communication is to be retained in pursuance of these Regulations.

Data to be retained: fixed network telephony

5. The following data must be retained as respects fixed network telephony—

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

(a) the calling telephone number;

(b) the name and address of the subscriber or registered user of any such telephone.

B. Data necessary to identify the destination of a communication:

(a) the telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred;

(b) the name and address of the subscriber or registered user of any such telephone.

C. Data necessary to identify the date, time and duration of a communication:

(a) the date and time of the start and end of the call.

D. Data necessary to identify the type of communication:

(a) the telephone service used.

Data to be retained: mobile telephony

6. The following data must be retained as respects mobile telephony—

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

(a) the calling telephone number;

(b) the name and address of the subscriber or registered user of any such telephone.

B. Data necessary to identify the destination of a communication:

(a) the telephone number dialled and, in cases involving supplementary services such as call forwarding or call transfer, any telephone number to which the call is forwarded or transferred;

(b) the name and address of the subscriber or registered user of any such telephone.

C. Data necessary to identify the date, time and duration of a communication:

(a) the date and time of the start and end of the call.

D. Data necessary to identify the type of communication:

(a) the telephone service used.

E. Data necessary to identify users' communication equipment (or what purports to be their equipment):

(a) the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI) of the telephone from which a telephone call is made;

(b) the IMSI and the IMEI of the telephone dialled;

(c) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the cell ID from which the service was activated.

F. Data necessary to identify the location of mobile communication equipment:

(a) the cell ID at the start of the communication;

(b) data identifying the geographic location of cells by reference to their cell ID.

Data to be retained: internet access, internet e-mail or internet telephony

7. The following data must be retained as respects internet access, internet e-mail or internet telephony—

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

(a) the user ID allocated;

(b) the user ID and telephone number allocated to the communication entering the public telephone network;

(c) the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.

B. Data necessary to identify the destination of a communication:

(a) in the case of internet telephony, the user ID or telephone number of the intended recipient of the call;

(b) in the case of internet e-mail or internet telephony, the name and address of the subscriber or registered user and the user ID of the intended recipient of the communication.

C. Data necessary to identify the date, time and duration of a communication:

(a) in the case of internet access—

(i) the date and time of the log-in to and log-off from the internet access service, based on a specified time zone,

(ii) the IP address, whether dynamic or static, allocated by the internet access service provider to the communication, and

(iii) the user ID of the subscriber or registered user of the internet access service;

(b) in the case of internet e-mail or internet telephony, the date and time of the log-in to and log-off from the internet e-mail or internet telephony service, based on a specified time zone.

D. Data necessary to identify the type of communication:

(a) in the case of internet e-mail or internet telephony, the internet service used.

E. Data necessary to identify users' communication equipment (or what purports to be their equipment):

(a) in the case of dial-up access, the calling telephone number;

(b) in any other case, the digital subscriber line (DSL) or other end point of the originator of the communication.

The retention period

8.—(1) The data specified in regulations 5 to 7 must be retained by the public communications provider until the end of the retention period.

(2) The retention period is—

(a) 12 months from the date of the communication in question, or

(b) such shorter period (not below 6 months) or longer period (not exceeding 24 months) from that date as may be specified by written notice given by the Secretary of State.

(3) Any such notice—

(a) must specify the public communications provider, or category of public communications providers, to whom it is given, and

(b) may specify different periods for different cases or classes of case or for different categories of data.

(4) The notice must be given or published in a manner the Secretary of State considers appropriate for bringing it to the attention of the public communications provider, or the category of providers, to whom it given.

Data protection and data security

9.—(1) Public communications providers must observe the following principles with respect to data retained in accordance with these Regulations—

(a) the retained data must be of the same quality and subject to the same security and protection as those data on the public electronic communications network;

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

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

(d) except in the case of data lawfully accessed and preserved, the data must be destroyed at the end of the retention period.

(2) It is the duty of the Information Commissioner, as the Supervisory Authority designated for the purposes of Article 9 of the Data Retention Directive, to monitor the application of the provisions of these Regulations with respect to the security of stored data.

(3) As regards the destruction of data at the end of the retention period—

(a) the duty of a public communications provider is to delete the data in such a way as to make access to the data impossible; and

(b) it is sufficient for a public communications provider to make arrangements for the operation of so deleting data to take place at such monthly or shorter intervals as appear to the provider to be convenient.

Access to retained data

10. Access to data retained in accordance with these Regulations may be obtained only—

(a) in specific cases, and

(b) in circumstances in which disclosure of the data is permitted or required by law.

Storage requirements for retained data

11. The data retained in pursuance of these Regulations must be retained in such a way that it can be transmitted without undue delay in response to requests.

Statistics

12.—(1) A public communications provider must provide the Secretary of State, as soon as practicable after 31st March in any year, with the following information in respect of the period of twelve months ending with that date.

(2) The information required is—

(a) the number of occasions when data retained in accordance with these Regulations have been disclosed in response to a request;

(b) the number of occasions when a request for lawfully disclosable data retained in accordance with these Regulations could not be met.

(3) The Secretary of State may, by notice given in writing to a public communications provider, vary the date specified in paragraph (1).

(4) The notice may contain such transitional provision as appears to the Secretary of State to be necessary in consequence of the variation.

Data retained by another communications provider

13.—(1) Except as provided by written notice given by the Secretary of State, these Regulations do not apply to a public communications provider if, or to the extent that, the communications data concerned are retained in the United Kingdom in accordance with these Regulations by another public communications provider.

(2) Any such notice must specify—

(a) the public communications provider, or category of public communications providers, to whom it is given, and

(b) the extent to which, and the date from which, the provisions of these Regulations are to apply.

(3) The notice must be given or published in a manner the Secretary of State considers appropriate for bringing it to the attention of the public communications provider, or the category of providers, to whom it given.

Reimbursement of expenses of compliance

14.—(1) The Secretary of State may reimburse any expenses incurred by a public communications provider in complying with the provisions of these Regulations.

(2) Reimbursement may be conditional on the expenses having been notified to the Secretary of State and agreed in advance.

(3) The Secretary of State may require a public communications provider to comply with any audit that may be reasonably required to monitor a claim for reimbursement.

Revocation

15.—(1) The Data Retention (EC Directive) Regulations 2007([3]), which are superseded by these Regulations, are revoked.

(2) Anything done under or for the purposes of those Regulations that could have been done under or for the purposes of the corresponding provision of these Regulations (if it had been in force at the time) shall be treated on and after these Regulations come into force as if it had been done under or for the purposes of that corresponding provision.

3 S.I. 2007/2199.

Home Office	Name
Date	Minister of State

EXPLANATORY NOTE

(This note is not part of the Order)

These Regulations implement Directive 2006/24/EC ("the Data Retention Directive") of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

The Data Retention (EC Directive) Regulations 2007 implemented the Data Retention Directive with respect to fixed network and mobile telephony. The United Kingdom made a declaration pursuant to Article 15.3 of the Data Retention Directive that it would postpone application of that Directive to the retention of communications data relating to internet access, internet telephony and internet e-mail. These Regulations implement the Data Retention Directive with respect to those forms of data, and revoke the Data Retention (EC Directive) Regulations 2007 which are superseded by these Regulations.

The Regulations impose a requirement on public communications providers ("providers"), as defined in regulation 2, to retain the categories of communications data specified in regulations 5, 6 and 7. The Regulations apply to all providers except as provided for in regulation 13. Regulation 4 makes provision regarding the obligation to retain the data specified in regulations 5, 6 and 7.

Such data must be retained, in accordance with regulation 8, for a period of 12 months, or for such shorter or longer period (not exceeding 24 months) as may be specified by written notice given by the Secretary of State . The data must be stored in accordance with the requirements in regulation 11, and may only be accessed in accordance with regulation 10.

Data protection and data security are provided for in regulation 9. Regulation 9(2) provides that the Information Commissioner, as the designated Supervisory Authority for the purposes of Article 9 of the Data Retention Directive, is responsible for monitoring the application of these Regulations with respect to the security of stored data.

There is a requirement on providers to provide statistics to the Secretary of State in regulation 12. Regulation 14 provides that the Secretary of State may make arrangements for reimbursing any expenses incurred by providers in complying with the Regulations.

ANNEX C

THE IMPACT ASSESSMENT

1. Title of proposal

1.1. Implementation of Directive 2006/24/EC (the Directive) on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

2. Purpose and intended effect

Objective

2.1. Through UK implementation of the Directive, the Government seeks to:

2.1.1. provide a legal framework for the retention of communications data to assist in the prevention, detection and prosecution of serious crime.

2.1.2. work with the European Commission and other Member States to encourage effective retention of communications data across the EU.

2.1.3. minimise the impact on the telecommunications industry whilst ensuring the necessary communications data is retained.

Background

2.2. The benefits of communications data to law enforcement and intelligence agencies have been recognised for a number of years. Increasingly, however, communications service providers are tending to retain less of this data as their business practices evolve. Additionally, data protection obligations have encouraged more efficient deletion of data that is no longer required for business purposes.

2.3. In the UK, Part 11 of the Anti-Terrorism, Crime and Security Act 2001 was introduced to enable Government to encourage communications service providers to retain communications data, even if there is no business purpose for doing so. This was implemented under a voluntary code of practice in 2003 and whilst many businesses already retain sufficient data, several providers were able to demonstrate that their communications data was being retained purely for Government purposes and were consequently reimbursed for associated costs.

2.4. Public Consultation on the voluntary code of practice for retention of Communications Data in 2003 demonstrated that the importance of this data is widely appreciated.

2.5. A number of public communications providers have indicated that they will not voluntarily comply with the code of practice and would prefer a mandatory framework; others have indicated that whilst they will comply voluntarily in the short term, they would prefer to be mandated in the future. S104 of the Anti-Terrorism, Crime and Security Act provides for subsequent secondary legislation to mandate providers to retain communications data, although this power will expire if it is not brought into force before December 2007.

2.6. Having established good foundations for retention of communications data in the UK, the Government pursued agreement across Europe by co-sponsoring a Framework Decision along with Ireland, France and Sweden in 2004. Later, the legal basis was changed to First Pillar Article 95 of the EC Treaty, resulting in this Directive in 2006. Ireland – along with Slovakia – opposed this change in legal basis, although the outcome of this legal challenge is unlikely to be known in advance of the implementation deadline.

Rationale for Government Intervention

2.7. Clearly, a key driver for this work is the need to complete the implementation of the European Directive. However, even in its absence, Government intervention would be required because of the need to evolve the voluntary code where it relates to internet-related data into a mandatory framework to ensure that this essential data is available regardless of providers' policies towards our voluntary approach.

2.8. During a two week survey in 2005 of data requirements placed by the police, there were 231 requests for data in the age category between 6 and 12 months old. 60% of these requests were in support of murder and terrorism investigations and 86% of the requests were for murder, terrorism and serious crime, which includes armed robbery and firearms offences. This highlights the significance of this older data which - without a mandatory framework for retention in place – is more at risk of deletion.

3. Consultation

3.1. We intend to hold a full Public Consultation on the draft Regulations. In advance of this, we have, when implementing the Electronic Communications Data Retention (EC Directive) Regulations 2007, continued our engagement with fixed and mobile telephone providers where they also provide internet services to their customers and have met on a regular basis with a range of trade associations and Government-Industry liaison groups.

3.2. We do not believe that these draft Regulations introduce any new privacy issues compared to the Data Retention (EC Directive) Regulations 2007[1] or the 2003 Voluntary Code of Practice under Part 11 of the Anti-Terrorism, Crime and Security Act 2001, and we will continue to engage with industry stakeholders before, during and after the public consultation process.

3.3. This Impact Assessment is also submitted as part of the Public Consultation.

1 See paragraph 1.7

4. Options

4.1. As always, it is necessary to consider the 'Do Nothing' approach. In addition to the need for Government Intervention to mitigate the risks associated with a decline in the available communications data, we have a commitment to implement this Directive as a Member State of the European Union. Failure to do so is likely to result in infraction proceedings.

4.2. The broad direction of the policy is set by the Directive. There are three key areas of flexibility:

4.2.1. the Directive does not comment on costs but the Commission made a declaration to the Council in February 2006 which acknowledged that retention of data may generate significant additional costs for communications providers and that reimbursement of demonstrated additional costs by Member States may be necessary. Therefore, there is a spectrum of options around funding from full funding by industry at one end, to full cost reimbursement by Government at the other, with a range of burden-sharing arrangements in between.

4.2.2. the Directive applies to the whole communication provider industry but within it, Recital 13 declares that data should be retained in such a way as to avoid their being retained more than once. We discussed this with the Commission in early January 2007 and again in 2008 and the Commission raised no concerns about interpreting this recital to minimise the impact on communication providers. A range of options are available which seek to capture the data required from different parts of the industry, attempting to minimise duplication whilst ensuring full coverage of communications data.

4.2.3. the Government must ensure that the data is retained for periods of not less than six months and not more than two years from the date of the communication.

4.3. As these dimensions are broadly independent – our choice of retention period, for example, can be considered separately from our choice of funding model – we identify below the best solution over each dimension in turn before combining these to generate a composite option which represents the optimal way to implement the Directive in the UK. This is then compared to the "do nothing" option to decide whether implementing the policy in this way is the right course of action.

Reimbursement of costs

4.4. The existing legislation in the UK on retention of internet-related data places a duty on the Secretary of State to ensure that arrangements are in force to make appropriate contributions towards communications providers who have incurred costs as a consequence of retaining communications data in accordance with the Act (Section 106 of ATCSA). However, given that the majority of other Member States have indicated that they do not intend to reimburse communications providers for additional costs, we must consider whether or not the UK should change its position with regard to this.

4.5. The retention work initially carried out under ATCSA has demonstrated that in order to realise the benefits of this data, it is important to invest in good retrieval systems where appropriate. Whilst the Directive includes an article requiring data to be transmitted without undue delay, we believe that a cooperative approach is the most effective way of ensuring effective retrieval systems are in place.

4.6. The reimbursement of costs would be restricted to expenditure that public communications providers have incurred by putting in place additional capability that is uniquely for the purpose of providing retention and disclosure of communications data to authorities empowered to access it under the Regulation of Investigatory Powers Act (RIPA) 2000.

4.7. The highly competitive market in the UK means that without reimbursing additional costs, those public communications providers receiving high volumes of disclosure requirements from RIPA authorities would be disadvantaged relative to other public communications providers in the UK.

4.8. Rather than reimbursing additional costs for retention and disclosure, or expecting industry to bear full costs of the proposals, we have also given thought to the option of requiring industry to bear the costs of retention but reimbursing additional costs for suitable retrieval solutions for those public communications providers who receive the highest volumes of requests. The work conducted under ATCSA and the Data Retention (EC Directive) Regulations 2007 suggests that retention and retrieval mechanisms are so intertwined that it would be difficult to introduce such measures without potentially introducing an advantage to public communications providers who receive the highest volumes of requests. This is because there is a risk that those providers who received funding for a suitable retrieval solution may unintentionally be subsidised for retention costs because it is difficult to separate this out from a retrieval solution.

4.9. To avoid the potential distortion of the UK market and to smooth the transition from our legislation under ATCSA (where it relates to the retention of internet-related data) to the draft Regulations that implement the final phase of the Directive, we propose that we continue reimbursing additional costs for both the retention and disclosure of all communications data.

Application of the Directive

4.10. The Directive applies to all public communications providers. However, within the Directive, Recital 13 declares that data should be retained in such a way as to avoid their being retained more than once. In order to avoid duplicative storage of data, we have identified the potential to interpret this to reduce the number of public communication providers required to retain communications data whilst continuing to aim for full retention of communications data in the UK. Our engagement with industry and law enforcement agencies has concluded that if more than one public communications service provider is in possession of particular communications data, then only one need retain the data for the purposes of the Directive, for example where a mobile network provider's services are sold by another provider, that provider will not be required to retain copies of itemised bills as that same detail will be retained within the scope of the Regulations by the mobile network provider. The European Commission has raised no concerns with this interpretation of Recital 13.

4.11. We expect this interpretation to reduce the number of public communications providers required to retain data because a significant proportion of the industry is involved in providing communications across networks owned by other communications providers. To reiterate the point, in such circumstances only one will need to retain the data and Government will continue to engage with industry and law enforcement to ensure matters are coordinated.

4.12. There are several reasons to seek to reduce the number of public communications providers who need to retain data subject to the Directive:

4.12.1. Minimising the number of public communications providers who are retaining the communications data will reduce the number of industry partners with whom the authorities requiring this data will need to interact. This will improve the efficiency of the disclosure process as it will result in a smaller pool of more experienced industry partners.

4.12.2. As recognised by the 2003 consultation paper on the Code of Practice for Voluntary Retention of Communications Data and our public consultation[2] on the initial transposition of the Directive, concerns may be raised under Article 8 (the right to respect for a person's private and family life, their home and correspondence) of the European Convention on Human Rights when considering retention of communications data. Article 8(2) of ECHR permits interference with individuals' right to privacy if it is in accordance with the law and is necessary in the interests of national security and the prevention and detection of crime. Such interference must also be proportionate. If it is possible to reduce duplicative storage of communications data, this should be done for the purposes of proportionality.

4.12.3. Reducing the number of public communications providers involved in retaining communications data will also minimise the costs associated with building specific storage and retrieval systems.

4.12.4. Variation in the number of public communications providers which must retain data is a primary determinant in the overall cost of implementing the Directive and is illustrated in the costs section below.

4.12.5. We propose that the most appropriate option is to continue to make provisions in the draft Regulations to enable public communications providers to avoid duplicative storage of data. This should minimise the number of public communications providers who are affected by these draft Regulations.

4.12.6. Because of the dynamic nature of the industry, there are difficulties associated with introducing definitions that subdivide the industry into a hierarchy that ensures communications data is only retained at the network level. The wording proposed for Regulation 3 is therefore the subject of question 1 in the consultation paper

2 See footnote 1

Period of Retention for communications data

4.13. The Directive provides flexibility with regard to the period for which communications data must be retained. Under our existing legislation (ATCSA), a retention period of 12 months was adopted. The 2003 consultation paper on the Code of Practice for Voluntary Retention of Communications Data considered three factors in assessing the proportionality of the retention period:

4.13.1. degree of intrusion involved into an individual's private life

4.13.2. strength of public policy justification

4.13.3. the adequacy of the safeguards in place to prevent abuse

4.14. The 2003 consultation paper concluded that 12 months is the optimal trade-off between law enforcement requirements and the associated interference with individuals' right to privacy. We do not believe that the period of time for which data must be retained is a significant driver of financial costs.

4.15. We do not believe that the proposed regulations alter the balance of these factors compared to the 2003 analysis.

Composite Option

4.16. Taking into account the optimisation of these different dimensions, our preferred option for recommendation is for a set of Regulations that:

4.16.1. allow Government to reimburse public communications providers for additional costs;

4.16.2. make provisions to avoid duplicative retention of communications data and

4.16.3. require communications data to be retained for a period of 12 months;

4.17. This preferred option, along with 'Do nothing' and an option identical except that it would not allow for the avoidance of duplicative retention of communications data, are illustrated in terms of costs and benefits in the table below. The issue of reimbursement is considered further under sections 5, 6 and 7.

4.18. Table – Costs and Benefits.

Options	Costs	Benefits/drawbacks
'Do nothing' continue with EU DRD fixed and mobile	• £3.5m capital • £7.75m resource over 8 years remain to be spent on EUDRD fixed and Mobile • This does not include an estimate for the cost of potential infraction proceedings.	• Some data will be available for the investigation, detection and prosecution of serious crime – but the data available will depend on the policy of individual businesses.
As above but proceed with ATCSA voluntary retention for internet	£25.65m capital, £12.23m resource over 8 years • This does not include an estimate for the cost of potential infraction proceedings.	• Appropriate data will be available to support the investigation, detection and prosecution of serious crime. • Infraction proceedings will not be avoided.
All public communications providers must retain data.	£68.44m capital, £39.40m resource over 8 years	• Appropriate data will be available to support the investigation, detection and prosecution of serious crime. • Infraction proceedings will be avoided.
Duplicative storage of communications data is avoided	£30.35m capital, £16.23m resource over 8 years EUDRD internet data retention including the cost of continuing with the fixed and mobile projects	• Appropriate data will be available to support the investigation, detection and prosecution of serious crime. • Infraction proceedings will be avoided.

5. Small firms impact test

5.1. Through reimbursing public communications providers for additional costs in complying with the proposed Regulations and by interpreting Recital 13 to minimise the number of public communications providers who must retain communications data, we believe that we will avoid a disproportionate impact on small firms.

6. Competition assessment

6.1. The proposed Regulations are designed to ensure that no public communications provider is either advantaged or disadvantaged by the requirements to retain communications data or the provisions for reimbursement of additional costs. Particular attention has been given to ensuring that the Secretary of State is able to fully audit payments made for additional costs to ensure that competition is not distorted and that there is no contravention of State Aid regulations. Consultation question 4 asks whether these measures will mitigate the impact on competition.

7. Enforcement, sanctions and monitoring

7.1. The Directive makes no provisions for imposing sanctions on those public communications providers who do not comply with the requirements. However, by adopting a cooperative approach whereby additional costs are paid to ensure that no public communications provider is disadvantaged by complying with our proposed Regulations, we believe that our measures will be sufficiently enforced. This assumption is supported by our experience of working cooperatively with industry under ATCSA and the Data Retention (EC Directive) Regulations 2007.

7.2. As part of our monitoring mechanisms to inform the annual reports to the Commission on the effectiveness of the implementation, we will seek to identify cases where requests for data could not be met. This data will inform the plans for completing the implementation of the Directive. If the statistics provide sufficient indication of non-compliance, we will review the need to introduce primary legislation to allow for the introduction of sanctions.

8. Implementation and delivery plan

8.1. We need to have appropriate legislation in place to take account of internet-related data by 15 March 2009. The draft Regulations will replace the Data Retention (EC Directive) Regulations 2007 and will incorporate the requirement for the retention of communications data in relation to fixed line telephony, mobile telephony, internet access, internet email and internet telephony.

8.2. The draft Regulations will apply throughout the United Kingdom.

9. Post-implementation review

9.1. Included in the Directive is a requirement to report annually to the Commission on:

9.1.1. the cases in which information was provided to the competent authorities in accordance with applicable national law,

9.1.2. the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,

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

9.2. The arrangements that we propose to put in place with industry will include the provision of statistics. Additionally, we will continue to record - on an exception basis - evidence from law enforcement and intelligence agencies to demonstrate both difficulties and benefits arising from these regulations.

10. Summary and recommendation

10.1. In the Government's assessment, the cost of imposing these requirements is justified by the benefits to society and our legal commitment to implement the EU Directive. By reimbursing industry for the burden that this would otherwise impose, the Government hopes to mitigate any potential competition and small business impacts and aims to ensure that it is funded in an equitable fashion.

10.2. On this basis, we recommend Government intervention to transpose the internet-related aspects of the Directive using Regulations under the European Communities Act of 1972. These Regulations should:

10.2.1. allow the Government to work cooperatively with the industry to ensure that appropriate retrieval mechanisms are in place;

10.2.2. make provisions to avoid duplicative retention of communications data and

10.2.3. require communications data to be retained for a period of 12 months;

10.3. Draft Regulations have been drafted in accordance with this option and are subject to public consultation alongside this Impact Assessment.

ANNEX D

PRELIMINARY SCREENING FOR EQUALITY IMPACT ASSESSMENT

PRELIMINARY SCREENING

This policy was screened for impact on equalities on 9 March 2007 and again on 28 July 2008. The following evidence has been considered. As a result of this screening, it has been decided that a full equality impact assessment is not required.

1. Communications data is usually already held by public communications providers for business purposes. The transposition of this Directive will ensure that the data is retained for long enough to support legitimate law enforcement and intelligence agency requirement.
2. The key difference between this policy and our original approach to retention of communications data is that these Regulations will mandate public communications providers to retain communications data for a minimum period. Our previous approach under Part 11 of the Anti-Terrorism, Crime and Security Act 2001, was to form voluntary relationships with public communications providers.
3. Because the proposed Regulations are only a change to an existing policy and because this approach will affect all users of communications in the same way, we do not believe that a full equality impact assessment is necessary.

ANNEX E

THE CONSULTATION CRITERIA

The six consultation criteria

1. Consult widely throughout the process, allowing a minimum of 12 weeks for written consultation at least once during the development of the policy.
2. Be clear about what your proposals are, who may be affected, what questions are being asked and the timescale for responses.
3. Ensure that your consultation is clear, concise and widely accessible.
4. Give feedback regarding the responses received and how the consultation process influenced the policy.
5. Monitor your department's effectiveness at consultation, including through the use of a designated consultation co-ordinator.
6. Ensure your consultation follows better regulation best practice, including carrying out a Impact Assessment if appropriate.

The full code of practice is available at:
http://www.berr.gov.uk/bre/consultation%20guidance/page44459.html

Consultation Coordinator

If you have any complaints or comments specifically about the consultation process only, you should contact the Home Office consultation co-ordinator Nigel Lawrence by email at: nigel.lawrence@homeoffice.gsi.gov.uk

Alternatively, you may wish to write to:
Nigel Lawrence
Consultation Co-ordinator
Performance and Delivery Unit
Home Office
3rd Floor Seacole
2 Marsham Street
London
SW1P 4DF