



Basic information	
2004/0813(CNS) CNS - Consultation procedure JHA act	Procedure lapsed or withdrawn
Combating crime: prevention of crime, criminal offences and terrorism, retention of data processed on public communications networks. Framework Decision. Initiative France, Ireland, Sweden and United Kingdom Subject 7.30.20 Action to combat terrorism 7.40.04 Judicial cooperation in criminal matters	

Key players					
European Parliament	Committee responsible		Rapporteur	Appointed	
	LIBE	Civil Liberties, Justice and Home Affairs	PICKART ALVARO Alexander Nuno (ALDE)	25/11/2004	
	Committee for opinion		Rapporteur for opinion	Appointed	
	ITRE	Industry, Research and Energy	The committee decided not to give an opinion.	27/01/2005	
	Committee for opinion on the legal basis		Rapporteur for opinion	Appointed	
	JURI	Legal Affairs	MEDINA ORTEGA Manuel (PSE)	21/09/2004	
	Council of the European Union	Council configuration		Meetings	Date
		Justice and Home Affairs (JHA)		2683	2005-10-12
		Justice and Home Affairs (JHA)		2664	2005-06-02
Justice and Home Affairs (JHA)		2626	2004-12-02		
European Commission	Commission DG		Commissioner		
	Justice and Consumers		FRATTINI Franco		

Key events			
Date	Event	Reference	Summary
28/04/2004	Legislative proposal published	08958/2004	Summary

01/12/2004	Committee referral announced in Parliament		
02/12/2004	Debate in Council		Summary
26/05/2005	Vote in committee		Summary
01/06/2005	Committee report tabled for plenary, 1st reading/single reading	A6-0174/2005	
02/06/2005	Debate in Council		Summary
07/06/2005	Results of vote in Parliament		
07/06/2005	Debate in Parliament	CRE link	Summary
27/09/2005	Decision by Parliament	T6-0348/2005	Summary
27/09/2005	Results of vote in Parliament		
12/10/2005	Debate in Council		Summary

Technical information	
Procedure reference	2004/0813(CNS)
Procedure type	CNS - Consultation procedure
Procedure subtype	Legislation
Legislative instrument	JHA act
Legal basis	Treaty on the European Union (after Amsterdam) M 031-p1-aa Treaty on the European Union (after Amsterdam) M 038 Treaty on the European Union (after Amsterdam) M 034-p2
Stage reached in procedure	Procedure lapsed or withdrawn
Committee dossier	LIBE/6/25028

Documentation gateway				
European Parliament				
Document type	Committee	Reference	Date	Summary
Committee opinion	JURI	PE355.785	08/04/2005	
Committee report tabled for plenary, 1st reading/single reading		A6-0174/2005	01/06/2005	
Text adopted by Parliament, 1st reading/single reading		T6-0348/2005 OJ C 220 21.09.2006, p. 0018-0045 E	27/09/2005	Summary
Council of the EU				
Document type	Reference	Date	Summary	
Legislative proposal	08958/2004	28/04/2004	Summary	

Additional information		
Source	Document	Date
European Commission	EUR-Lex	

Combating crime: prevention of crime, criminal offences and terrorism, retention of data processed on public communications networks. Framework Decision. Initiative France, Ireland, Sweden and United Kingdom

2004/0813(CNS) - 27/09/2005 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted a resolution drafted by Alexander Nuno ALVARO (ALDE, DE) definitively rejecting the initiative of France, Ireland, Sweden and the United Kingdom. (Please see the summary of the plenary debate of 07/06/2005.) and referred the report back to the Civil Liberties Committee. In its 27 September 2005 vote, the European Parliament reconfirmed its rejection of this initiative. As a result, this procedure has reached its conclusion. From this date on, Members will examine a new proposal for a Directive from the Commission covering the same subject and involving the Parliament in the co-decision procedure thus giving it a stronger position (please refer to 2005/0182/COD).

The proposed framework decision supported by the UK Presidency of the Union had become one of its main priorities since the London bombs in July. The Presidency will again be able to draw support for its proposal from the same Member States in the weeks to come.

Combating crime: prevention of crime, criminal offences and terrorism, retention of data processed on public communications networks. Framework Decision. Initiative France, Ireland, Sweden and United Kingdom

2004/0813(CNS) - 12/10/2005

The Council held an exchange of views on the basis of a paper from the Presidency.

A large number of delegations could accept the elements set out by the Presidency paper as the basis for further work, subject to maintaining the derogation in Article 15(1) of the 2002 telecommunications Directive and clarifying its future scope.

In the next stage, the Framework Decision will remain on the table, as an option favoured by a large number of delegations. However, a majority of delegations were also open to the idea of adopting a Directive.

There was wide agreement that any measure must reflect the elements referred to in the Presidency paper, notably in respect of the provisions on retention periods, scope and costs.

The Council agreed that work should be taken forward urgently. It instructed Coreper to finalise agreement on all outstanding issues as soon as possible, and agreed that informal contacts with the European Parliament should continue in order to maximise common ground between the Council and the EP on issues of substance, while respecting the Council's position as set out above. The Council agreed to revert to this issue at its next meeting with a view to a final decision before the end of the year.

It should be noted that a proposal on data retention was made in April 2004 by France, Ireland, Sweden and the UK, on the basis of Articles 31 and 34 of the Treaty of the European Union, under the so-called "Third Pillar". For it to be adopted, such a proposal needs unanimity at Council level.

However, the Commission has taken the view that the categories of data to be retained and the period for retaining such data fall within EC competence ("First Pillar") and should be adopted by the Council in codecision with the European Parliament, on the basis of a Commission proposal for a Directive. On 21 September 2005 the Commission adopted such a proposal for a Directive on retention of communication data.

Combating crime: prevention of crime, criminal offences and terrorism, retention of data processed on public communications networks. Framework Decision. Initiative France, Ireland, Sweden and United Kingdom

2004/0813(CNS) - 02/06/2005

The Council held an exchange of views on certain key issues concerning this issue and in particular the list of data to be retained, the length of the retention period, and the legal basis for the act.

The Presidency concluded that delegations could agree on a course of action and certain key elements of the Framework Decision:

- data retention is an important element in the fight against crime and terrorism, and an EU legislative act is needed;
- to reach rapid agreement on this Framework Decision, a gradual approach to the issue would be preferable, beginning with the retention of data on fixed and mobile telephone communication;

- those Member States which are not immediately able to collect data concerning the internet, and in the area of telephony, data concerning unsuccessful outgoing calls may have a transitional period for application of the Framework Decision, to be time-limited for a period which has not yet been determined;
- communications service providers and judicial investigation departments will be consulted to consider the costs of implementing this Framework Decision, amongst other matters;
- regarding the list of communication data to be retained, in general delegations were able to accept the Presidency's approach, which provides for a minimum list of data to be retained. This list should be mainly functional, with some technical specifications concerning different types of telecommunications;
- most delegations were able to accept the timelines laid down in the Presidency compromise text: the normal duration of the data retention period would be twelve months. The Member States would be authorised to provide for a shorter period in exceptional circumstances, which could, however, not be less than six months;
- the majority of delegations believed that the legal basis for the proposal should be Title VI of the TEU (Article 31(1), point (c), and Article 34(2), point (b)).

This item will be addressed again at the informal meeting of Ministers for Justice and Home Affairs to take place in September under the United Kingdom Presidency.

Combating crime: prevention of crime, criminal offences and terrorism, retention of data processed on public communications networks. Framework Decision. Initiative France, Ireland, Sweden and United Kingdom

2004/0813(CNS) - 28/04/2004 - Legislative proposal

PURPOSE : to facilitate criminal co-operation by approximating Member States' legislation on the retention of data processed and stored by providers of publicly available electronic communications or networks.

PROPOSED ACT : Framework Decision.

CONTENT : this Framework Decision is being proposed on the initiative of the French Republic, Ireland, the Kingdom of Sweden and the United Kingdom. In its pre-amble the Decision notes that whilst certain Member States are forging ahead with legislation relating to the retention of data, this legislation is disparate, thus hindering co-operation in the prevention of criminal activities involving electronic data. Setting parameters and ensuring that all Member States take the necessary steps to retain certain types of data for a uniform length of time will help prevent criminal offences - including terrorist activities.

The Decision is being proposed within the context of the EU's commitment to create an area of liberty, security and justice. It also refers to the Parliamentary resolution of May 2000, which calls for greater intervention in the area of high-tech crime. Specifically speaking, the proposal relates only to data generated as a result of communications and does not relate to data that is the content of the information communicated. The Decision draws a distinction between the "retention" of data – which will fall under the provisions of this Framework Decision and the "preservation" of data, which will not. Essentially, the Council is seeking to retain data in order to trace the source of illegal content such as child pornography and racist and xenophobic material as well as being able to source attacks against information systems and to identify those involved in using electronic communications networks for the purpose of organised crime and terrorism. For example, the kind of data which will need to be retained includes processed and stored bills for commercial purposes. On the other hand, the Decision does not apply to data retention relating to national or state security, defence or public security. Nor, does the Framework Decision apply to access to data at the time of transmission – that is by monitoring, intercepting or recording telecommunications. Further, the Decision specifies that the retention of data must be proportionate to the needs of prevention and detection compared to an individual's right to privacy. In summary, the provisions outlined in the Decision are as follows:

Scope and Aim: The aim of the Framework Decision is to facilitate judicial co-operation in criminal matters by approximating Member States' legislation on the retention of data processed and stored by providers of publicly available electronic communications services or networks. It will not apply to the content of exchanged communications

Definitions: Traffic data and subscriber information are defined and fall under the Framework Decision's scope. The data covered by the Decision relates to all data necessary to trace and identify the source of a communication, to identify the routing and destination of a communication, to identify the time, date and duration of a communication, to identify the telecommunication, to identify the communication device and lastly to identify the location at the start and throughout the duration of the communication. Data can be generated by services including, inter alia, telephony, electronic media services, internet protocols such as e-mails, voice over internet protocols, the world wide web, subsets of internet protocols etc.

Retention of data: Member States must take the necessary measures to retain the data processed and stored by providers of a public communications network and to ensure that the information retained is in accordance with the provisions of the Framework Decision.

Time period for the retention of data: Data shall be retained for a period of at least 12 months and not more than 36 months following its generation. Member States, may under certain conditions, derogate from this provisions. In which case they must inform the Council and the Commission its reasons for wishing to do so.

Access to data: Member States may request access to data in accordance with procedures adopted for judicial co-operation in criminal matters.

Data Protection: Principles have been enshrined in the Framework Decision to ensure that data is protected and the data retained is set to a minimum for the purposes of crime prevention and detection. For example, data may only be accessed for specific, explicit and legitimate purposes by the competent authorities. In addition the data should be relevant and not excessive, the confidentiality and integrity of the data must be ensured and the data accessed must be accurate.

Data security: Member States must ensure that the data retained is subject to certain basic security measures. For example, the retained data shall be of the same quality as the data already on the network, data must be protected against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access and against all other unlawful forms processing. Moreover, data must be destroyed at the end of the period for retention.

Implementation: Member States must have measures in place to comply with the Framework Decision within two years following the date of adoption.

Combating crime: prevention of crime, criminal offences and terrorism, retention of data processed on public communications networks. Framework Decision. Initiative France, Ireland, Sweden and United Kingdom

2004/0813(CNS) - 02/12/2004

The Council examined the scope of the draft Framework Decision on data retention. To recall, the proposal implies in principle that providers of publicly available electronic communications services or networks must retain specified data enabling the source, routing, destination, time, date and duration of communications and the location of the telecommunications devices used to be established. In its original form, the proposal seems to be limited to data already processed and stored for billing, commercial and other legitimate purposes.

However, this approach would imply that the possibilities for access to data for law enforcement purposes depend on the technical and commercial setup of each individual service provider. Some service providers apply systems, such as flat-rate systems, which imply that relevant data, processed for the purpose of providing the telecommunication concerned, are erased immediately after the communication has been terminated.

The Council therefore instructed its preparatory bodies to examine another approach entailing an obligation for service providers to retain relevant data defined in a common list in the instrument, provided that the data are processed/generated by the service provider in the process of supplying the telecommunications service concerned. Particular consideration should be given to the proportionality of the measure in relation to costs, privacy (data protection) and efficiency.

This approach may lead to a higher degree of certainty for the retention of the data concerned, and is less sensitive to the commercial behaviour of the service provider and technical developments. The service provider would be under an obligation to retain the data concerned to the extent that the data are processed/generated by the service provider, even if the data have no interest for the service provider. The level of harmonisation of Member States' legislation would be relatively high. Judicial authorities and law enforcement authorities have during the last years increasingly expressed concerns regarding the use of technical innovations, brought about by the continuous development of electronic telecommunications services, for the purpose of committing crimes, and the difficulties which this may cause regarding detection of and investigation into crimes. These concerns relate not only to communications by fixed phones, mobile phones, short message services (SMS), electronic media services (EMS) and multi media services (MMS). Increasingly, they also relate to Internet Protocols including email, voice over the Internet, worldwide web, file transfer protocols, network transfer protocols, voice over broadband, etc.