EUROPEAN PARLIAMENT

2004 *2009*

Session document

FINAL
A6-0205/2007

24.5.2007

*

REPORT

on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (renewed consultation)
(7315/2007 – C6-0115/2007 – 2005/0202(CNS))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Martine Roure

PR_CNS_art93am

Symbols for procedures

*	Consultation procedure *majority of the votes cast*
**I	Cooperation procedure (first reading) *majority of the votes cast*
**II	Cooperation procedure (second reading) *majority of the votes cast, to approve the common position* *majority of Parliament's component Members, to reject or amend the common position*
***	Assent procedure *majority of Parliament's component Members except in cases covered by Articles 105, 107, 161 and 300 of the EC Treaty and Article 7 of the EU Treaty*
***I	Codecision procedure (first reading) *majority of the votes cast*
***II	Codecision procedure (second reading) *majority of the votes cast, to approve the common position* *majority of Parliament's component Members, to reject or amend the common position*
***III	Codecision procedure (third reading) *majority of the votes cast, to approve the joint text*

(The type of procedure depends on the legal basis proposed by the Commission.)

Amendments to a legislative text

In amendments by Parliament, amended text is highlighted in ***bold italics***. Highlighting in *normal italics* is an indication for the relevant departments showing parts of the legislative text for which a correction is proposed, to assist preparation of the final text (for instance, obvious errors or omissions in a given language version). These suggested corrections are subject to the agreement of the departments concerned.

CONTENTS

Page

DRAFT EUROPEAN PARLIAMENT LEGISLATIVE RESOLUTION

on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (7315/2007 – C6-0115/2007 – 2005/0202(CNS))

(Consultation procedure - renewed consultation)

The European Parliament,

– having regard to the Council proposal (7315/2007),

– having regard to the Council's amendments (7315/1/2007),

– having regard to the Commission proposal (COM(2005)0475),

– having regard to its position of 27 September 2006[1],

– having regard to Articles 30, 31 and 34(2)(b) of the Treaty on European Union,

– having regard to Article 39(1) of the Treaty on European Union, pursuant to which the Council consulted Parliament again (C6-0115/2007),

– having regard to Rules 93, 51 and 55(3) of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A6-0205/2007),

1. Approves the Council proposal as amended;

2. Calls on the Council to amend the text accordingly;

3. Calls on the Council to notify Parliament if it intends to depart from the text approved by Parliament;

4. Asks the Council to consult Parliament again if it intends to amend its proposal substantially;

5. Strongly regrets the lack of consensus in the Council on an extended scope for the Framework Decision, and calls on the Commission and the Council to propose the extension of its scope to data processed at national level after the assessment and revision of the Framework Decision and at the latest three years after its entry into force in order to ensure the coherence of data protection rules in the European Union;

6. Calls on the Council and Commission formally to endorse the fifteen principles relating to the protection of personal data processed in the framework of police and judicial cooperation in criminal matters;

[1] Texts Adopted on that date, P6_TA(2006)0370.

7. Instructs its President to forward its position to the Council and Commission.

Text proposed by the Commission	Amendments by Parliament

Amendment 1
Recital 7 a (new)

	(7a) This Framework Decision should not be interpreted as a measure requiring Member States to reduce the level of protection resulting from national provisions intended to extend the principles laid down in Directive 95/46/EC to the field of judicial and police cooperation.

Justification

In the data protection sphere, as in other areas relating to the protection of fundamental rights, EU legislation must under no circumstances serve as an opportunity to reduce the level of protection already in place within Member States.

Amendment 2
Recital 10 a (new)

	(10a) With reference to 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[1], which provides for data stored by private persons to be made available for the investigation, detection and prosecution of serious offences, there should be a minimum degree of harmonisation of the obligations of private individuals persons processing data when carrying out a public service remit; the rules permitting access to such data by the competent authorities of a Member State should also

be harmonised.

[1] OJ L 105 of 13.4.2006, p. 54.

Justification

When Directive 2006/24/EC was adopted, the Council gave a moral commitment to ensuring that minimum rules on private persons processing data when carrying out a public-service remit were adopted in this Framework Decision.

Amendment 3
Recital 12

(12) Where personal data are transferred from a Member State of the European Union to third countries or international bodies, these data ***should, in principle,*** benefit from an adequate level of protection.	(12) Where personal data are transferred from a Member State of the European Union to third countries or international bodies, these data ***must*** benefit from an adequate level of protection.

Justification

Data cannot be exchanged with a third country unless the latter provides guarantees of an adequate level of protection.

Amendment 4
Recital 13

(13) ***It may be necessary to inform*** data subjects regarding the processing of their data, in particular where there has been particularly serious encroachment on their rights as a result of secret data collection measures, in order to ensure that data subjects can have effective legal protection.	(13) Data subjects ***should, without fail, be informed of*** the processing of their data, in particular where there has been particularly serious encroachment on their rights as a result of secret data collection measures, in order to ensure that data subjects can have effective legal protection.

Justification

Individuals have an alienable right to be notified if their personal data are used. This is a fundamental principle of data protection that must be upheld (see Principle 7 - information to be given to the data subject).

Amendment 5
Recital 14

(14) ***In order to ensure the protection of personal data without jeopardising the purpose of criminal investigations, it is necessary to define the rights of the data subject.***	(14) ***It is necessary to define the rights of the data subject, in order to ensure the protection of personal data without jeopardising the purpose of criminal investigations.***

Justification

The emphasis should be on protection of the data subject.

Amendment 6
Recital 15

(15) It is appropriate to establish common rules on the confidentiality and security of the processing, on liability and sanctions for unlawful use by competent authorities as well as judicial remedies available for the data subject. It is, however, for each Member State to determine the nature of its tort rules and of the sanctions applicable to violations of domestic data protection provisions.	(15) It is appropriate to establish common rules on the confidentiality and security of the processing, on liability and sanctions for unlawful use by competent authorities as well as judicial remedies available for the data subject. It is, however, for each Member State to determine the nature of its tort rules and of the sanctions***, including penal sanctions***, applicable to violations of domestic data protection provisions

Amendment 7
Recital 16

(16) The ***establishment*** in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of personal data processed in the framework of police and judicial cooperation between the Member States.	(16) The ***appointment*** in Member States of ***national*** supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of personal data processed in the framework of police and judicial cooperation between the Member States. ***The functions provided for in Article 25 of this Framework Decision should be assigned to the national data protection authorities established in accordance with Article 28 of Directive 95/46/EC.***

Justification

In order to ensure the fullest and most effective supervision, it is important not to establish more than one data protection authority within the same country.

Amendment 8
Recital 17

(17) Such authorities should have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings. These authorities should help to ensure transparency of processing in the Member States within whose jurisdiction they fall. However, their powers should not interfere with specific rules set out for criminal proceedings or the independence of the judiciary.	(17) Such authorities should have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to ***initiate and otherwise*** engage in legal proceedings. These authorities should help to ensure transparency of processing in the Member States within whose jurisdiction they fall. However, their powers should not interfere with specific rules set out for criminal proceedings or the independence of the judiciary.

Amendment 9
Recital 18

(18) The Framework Decision also aims to combine the ***existing*** data protection supervisory bodies, which have hitherto been established separately for the Schengen Information System, Europol, Eurojust, and the third-pillar Customs Information System, into a single data protection supervisory authority. A single supervisory authority should be created, which ***could, where appropriate***, also act in an advisory capacity. A single supervisory authority allows the improvement in third-pillar data protection to be taken a decisive step further	(18) The Framework Decision also aims to combine the data protection supervisory bodies ***in existence at European level***, which have hitherto been established separately for the Schengen Information System, Europol, Eurojust, and the third-pillar Customs Information System, into a single data protection supervisory authority. A single supervisory authority should be created, which ***should***, where appropriate, also act in an advisory capacity. A single supervisory authority allows the improvement in third-pillar data protection to be taken a decisive step further.

Justification

The aim is not to combine the various national supervisory bodies. This needs to be made clear.

Amendment 10
Recital 18 a (new)

(18a) A joint supervisory authority should gather the national supervisory authorities and the European Data Protection Supervisor.

Justification

The joint supervisory authority established under this Framework Decision should combine the national supervisory authorities of each Member State and the European authority in this area.

Amendment 11
Recital 22

(22) It is appropriate that this Framework Decision also applies to the personal data which are processed in the framework of the second generation of the Schengen Information System and the related exchange of supplementary information pursuant to Decision JHA/2006/ …on the establishment, operation and use of the second generation Schengen Information System.	(22) It is appropriate that this Framework Decision also applies to the personal data which are processed in the framework of the second generation of the Schengen Information System and the related exchange of supplementary information pursuant to Decision JHA/2006/ …on the establishment, operation and use of the second generation Schengen Information System ***and in the context of the Visa Information System pursuant to Decision JHA/2006/... on access for consultation purposes to the Visa Information System (VIS) by the competent authorities of the Member States and by Europol***.

Justification

A reference to the VIS needs to be inserted so as to ensure that this Framework Decision also applies to access to the visa information system by the authorities responsible for internal security.

Amendment 12
Recital 25 a (new)

(25a) With a view to ensuring that the international obligations of the Member States are fulfilled, this Framework

Decision may not be interpreted as guaranteeing a level of protection lower than that resulting from Convention 108 of the Council of Europe and the Additional Protocol thereto or from Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms or the case-law relating thereto. Similarly, in keeping with Article 6(2) of the Treaty on European Union and the Charter of Fundamental Rights of the European Union, with particular reference to Articles 1, 7, 8 and 47 thereof, the interpretation of the level of protection laid down by this Framework Decision must be the same as that laid down by those two Conventions.

Justification

This Framework Decision must not provide for a lower level of data protection than that currently in place under Council of Europe Convention 108.

Amendment 13
Recital 26 a (new)

(26a) This Framework Decision is merely the first step towards a more comprehensive and consistent framework for the protection of personal data used for security purposes. Such a framework may be based on the principles attached to this Framework Decision.

Justification

Parliament has for several years been asking the Council to adopt common principles on the protection of data used for security purposes. The rapporteur endorses the 15 principles and calls on the other European institutions to follow suit.

Amendment 14
Recital 32

(32) This Framework Decision respects the fundamental rights and observes the principles recognised in particular by the	(32) This Framework Decision respects the fundamental rights and observes the principles recognised in particular by the

Charter of Fundamental Rights of the European Union. This Framework Decision seeks to ensure full respect for the rights to privacy and the protection of personal data in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.	Charter of Fundamental Rights of the European Union. This Framework Decision seeks to ensure full respect for the rights to privacy and the protection of personal data in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, ***which are specific expressions of the right to human dignity enshrined in Article 1 of the Charter, Article 47 of which also guarantees the right to an effective remedy and to a fair trial***.

Amendment 15
Article 1, paragraph 1

1. The purpose of this Framework Decision is to ensure a high level of protection of the ***basic*** rights and freedoms, and in particular the privacy, of individuals with regard to the processing of personal data in the framework of police and judicial cooperation in criminal matters, provided for by Title VI of the Treaty on European Union, ***while guaranteeing a high level of public safety.***	1. The purpose of this Framework Decision is to ensure a high level of protection of the ***fundamental*** rights and freedoms, and in particular the privacy, of individuals with regard to the processing of personal data in the framework of police and judicial cooperation in criminal matters, provided for by Title VI of the Treaty on European Union.

Amendment 16
Article 1, paragraph 4

4. Authorities or other offices dealing specifically with matters of national security do not fall within the scope of this Framework Decision.	***deleted***

Justification

The Framework Decision should apply to all national authorities, without exception.

Amendment 17
Article 1, paragraph 2

2. The Member States and institutions and bodies established on the basis of Council	2. The Member States and institutions and bodies established on the basis of Council

acts pursuant to Title VI of the Treaty on European Union shall, by compliance with this Framework Decision, guarantee that the ***basic*** rights and freedoms, and in particular the privacy, of data subjects are fully protected when personal data are transmitted between Member States or institutions and bodies established on the basis of Council acts pursuant to Title VI of the Treaty on European Union for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or further processed for the same purpose by the recipient Member State or institutions and bodies established on the basis of Council acts pursuant to Title VI of the Treaty on European Union.	acts pursuant to Title VI of the Treaty on European Union shall, by compliance with this Framework Decision, guarantee that the ***fundamental*** rights and freedoms, and in particular the privacy, of data subjects are fully protected when personal data are transmitted between Member States or institutions and bodies established on the basis of Council acts pursuant to Title VI of the Treaty on European Union for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, or further processed for the same purpose by the recipient Member State or institutions and bodies established on the basis of Council acts pursuant to Title VI of the Treaty on European Union.

Amendment 18
Article 1, paragraph 5 a (new)

	5a. No later than three years after the date of entry into force of this Framework Decision, the Commission may submit proposals with a view to extending its scope to cover the processing of personal data within the framework of police and judicial cooperation at national level.

Justification

Extending the Framework Decision's scope to cover all data processed within the Member States is a priority with a view to ensuring a harmonised level of data protection. In the absence of agreement on this matter within the Council, this amendment provides for it to be discussed again in the medium term.

Amendment 19
Article 2, point (g)

(g) "the data subject's consent" shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to	***deleted***

him being processed;

Justification

Data subjects rarely have a proper chance freely to give their consent, since refusing to do so has negative repercussions in most cases. It is thus unrealistic to assume that private individuals can freely consent to their data being processed.

Amendment 20
Article 2, point (k)

k) "to make anonymous" shall mean to modify personal data in such a way that details of personal or material circumstances can no longer ***or only with disproportionate investment of time, cost and labour*** be attributed to an identified or identifiable individual.	k) "to make anonymous" shall mean to modify personal data in such a way that details of personal or material circumstances can no longer be attributed to an identified or identifiable individual.

Amendment 21
Article 3, paragraph 1

1. Personal data may be collected by the competent authorities only for the lawful purposes established explicitly pursuant to Title VI of the Treaty on European Union and may be processed only for the same purpose for which the data were collected. Processing of the data must be ***essential and*** appropriate to this purpose, ***and must not be excessive.***	1. Personal data may be collected by the competent authorities only for the lawful purposes established explicitly pursuant to Title VI of the Treaty on European Union and may be processed ***fairly and lawfully*** only for the same purpose for which the data were collected. Processing of the data must be ***necessary,*** appropriate ***and proportionate*** to this purpose.

Amendment 22
Article 3, paragraph 1 a (new)

	1a. Personal data shall be evaluated taking into account their degree of accuracy or reliability, their source, the categories of data subjects, the purposes for which they are processed and the phase in which they are used. Data which are inaccurate or incomplete shall be erased or rectified.

Amendment 23
Article 3, paragraph 1 b (new)

1b. Data mining and any form of large-scale processing of massive quantities of personal data, in particular where related to non-suspects, including the transfer of such data to a different controller, shall be permitted only if carried out in compliance with the results of an examination performed by a supervisory authority either prior to the start thereof or in the context of the preparation of a legislative measure.

Justification

All necessary precautions must be taken when processing data (see Principle 5 - data quality).

Amendment 24
Article 3, paragraph 1 c (new)

1c. Personal data shall be processed by separating facts and objective evaluations from opinions or personal assessments, and the data relating to the prevention and prosecution of offences from data lawfully held for administrative purposes.

Justification

Data must be processed in an objective manner (see Principle 5 - data quality).

Amendment 25
Article 3, paragraph 2, point (c)

c) processing is ***essential and*** appropriate to that purpose.	c) processing is ***necessary***, appropriate ***and proportional*** to that purpose.

Amendment 26
Article 4, paragraph 1 a (new)

1a. Member States shall ensure that the quality of personal data made available to the competent authorities of other Member States is verified regularly in order to ensure that the data accessed are accurate and up to date. Member States shall ensure that personal data that are no longer accurate or up to date are neither transferred nor made available.

Justification

Member States must take all necessary steps to ensure that the data transmitted are reliable.

Amendment 27
Article 7

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life ***shall be permitted only when this is strictly necessary and when suitable additional safeguards are provided.***	The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life ***shall be prohibited.***
	By way of exception, the processing of such data may be carried out:
	- if the processing is provided for by law, following prior authorisation by a competent judicial authority, on a case-by-case basis and is absolutely necessary for the prevention, investigation, detection or prosecution of terrorist offences and of other serious criminal offences,
	- if Member States provide for suitable specific safeguards, for example access to the data concerned only for personnel who are responsible for the fulfilment of the legitimate task that justifies the processing.
	These specific categories of data may not

be processed automatically unless domestic law provides appropriate safeguards. The same condition shall apply to personal data relating to criminal convictions.

Amendment 28
Article 7, paragraph 1 a (new)

1a. Appropriate safeguards shall be provided for by specific provisions, or on the basis of prior checking, in respect of processing operations that are likely to present specific risks to the rights and freedoms of data subjects, such as in particular the processing of DNA profiles, biometric data, data of non-suspects and the use of particular surveillance techniques or new technologies.

Justification

Data processing should be strictly regulated in accordance with Article 6 of Convention 108 (see Principle 6 - special categories of data).

Amendment 29
Article 10, paragraph 1

1. The transmitting body shall, upon transmission of the data, indicate the time-limits for the retention of data provided for under its national law, following the expiry of which the recipient must also erase the data or review whether or not they are still needed. Irrespective of these time-limits, transmitted data must be erased once they are no longer required for the purpose for which they were transmitted or for which they were allowed to be further processed in accordance with Article 11.	1. The transmitting body shall, upon transmission of the data, indicate the time-limits for the retention of data provided for under its national law, following the expiry of which the recipient must also erase the data or review whether or not they are still needed ***for the specific case for the purpose of which they were transmitted and must inform the supervisory authority and the transmitting body***. Irrespective of these time-limits, transmitted data must be erased once they are no longer required for the purpose for which they were transmitted or for which they were allowed to be further processed in accordance with Article 11.

Amendment 30
Article 11, paragraph 1

11. All transmissions of personal data are to be logged or documented for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security.	11. All transmissions of personal data are to be logged or documented for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security**,** ***as is all access to such data***.

Justification

Article 11, in order to be effective for the purposes of verification of the lawfulness of data processing, shall lay down appropriate mechanisms for logging or documenting not only all transmissions of data, but also all accesses to data.

Amendment 31
Article 12, paragraph 1, introduction

1. Personal data received from or made available by the competent authority of another Member State may be further processed only for the following purposes other than those for which they were transmitted:	1. Personal data received from or made available by the competent authority of another Member State may be further processed only for the following purposes other than those for which they were transmitted ***and only subject to the provisions of national law***:

Justification

The processing of data for purposes other than those for which they were collected cannot be carried out unless such processing is permissible under national law.

Amendment 32
Article 12, paragraph 1, point (a)

(a) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted or made available;	(a) the prevention, investigation, detection or prosecution of criminal offences ***in the same field*** or the execution of criminal penalties other than those for which they were transmitted or made available;

Justification

Personal data may only be used for the prosecution of criminal offences if the offence is linked to the purpose for which the data were originally collected.

Amendment 33
Article 12, paragraph 1, point (d)

(d) any other purpose only with the prior consent of the competent authority that has transmitted or made available the personal data, ***unless the competent authority concerned has obtained the consent of the data subject,***	(d) any other ***specified*** purpose***, provided that it is legitimate and not excessive in relation to the purposes for which they were registered in accordance with Article 5 of Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter referred to as "Convention 108"), but*** only with the prior consent of the competent authority that has transmitted or made available the personal data,

Justification

It is necessary to regulate strictly the subsequent processing of data for purposes different to those for which the data were collected. The possibility of such processing if the person concerned gives consent for it should be deleted, because such consent is rarely given freely, as a refusal will in most cases have adverse consequences for the data subject.

Amendment 34
Article 12, paragraph 1, last subparagraph

and where the requirements of Article 3(2) are met. The competent authorities may also use the transmitted personal data for historical, statistical or scientific purposes, provided that Member States ***provide appropriate safeguards, such as, for example, making*** the data anonymous.	and where the requirements of Article 3(2) are met. The competent authorities may also use the transmitted personal data for historical, statistical or scientific purposes, provided that Member States ***make*** the data anonymous.

Amendment 35
Article 12, paragraph 2

2. ***In cases where appropriate conditions are laid down for the processing of personal data on the basis of Council acts in accordance with Title VI of the Treaty on European Union, these conditions shall take precedence over paragraph 1.***	2. ***Exceptions subsequent to the date of entry into force of this Framework Decision other than those indicated in paragraph 1 shall be permitted only in extraordinary cases, on the basis of a specific, duly substantiated decision of the Council after consultation of the European Parliament.***

Justification

This Framework Decision is intended to apply to the whole of the third pillar. Different provisions on data protection can only be adopted in exceptional cases.

Amendment 36
Article 13

The transmitting authority shall inform the recipient of processing restrictions applicable under its national law to data exchanges between competent authorities within that Member State. The recipient must also comply with these processing restrictions.	The transmitting authority shall inform the recipient of processing restrictions applicable under its national law to data exchanges between competent authorities within that Member State. The recipient must also comply with these processing restrictions ***or apply its own national law if the latter affords greater protection***.

Amendment 37
Article 14

Personal data received from or made available by the competent authority of another Member State may be transferred to third States or international bodies only if the competent authority of the Member States which transmitted the data has given its consent to transfer in compliance with its national law.	***Member States shall provide that personal data may be transferred to third countries or international bodies or organisations established by international agreements or declared as an international body only if***
	(a) such transfer is necessary for the prevention, investigation, detection or prosecution of terrorist offences and of other serious criminal offences,
	(b) the receiving authority in the third country or receiving international body or organisation is responsible for the prevention, investigation, detection or prosecution of criminal offences,
	(c) the Member State from which the data were obtained has given its consent to the transfer in compliance with its national law, and
	(d) the third country or international body concerned ensures an adequate level of protection for the intended data

processing pursuant to Article 2 of the Additional Protocol to the Council of Europe Convention of 28 January 1981 for the Protection of individuals with regards to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, and the corresponding case-law pursuant to Article 8 of the ECHR.

Member States shall ensure that records are kept of such transfers and make them available to national data protection authorities on request.

Amendment 38
Article 14, paragraph 1 a (new)

1a. The Council, acting on the basis of an opinion delivered by the joint supervisory authority provided for in Article 26, and after consulting the Commission and the European Parliament, may establish that a third country or an international body ensures an adequate level of protection of privacy and of the fundamental freedoms and rights of the individual by virtue of its domestic legislation or international agreements.

Justification

Under the Additional Protocol to Convention 108, Member States are required to guarantee an adequate level of protection of data in their exchanges with third countries.

Amendment 39
Article 14, paragraph 1 b (new)

1b. By way of exception, but in accordance with the principles of jus cogens, personal data may be communicated to the competent authorities of third countries or to international bodies which do not ensure an adequate level of protection or where this level of protection is not ensured, in

case of absolute necessity in order to safeguard the essential interests of a Member State or for the purpose of averting imminent serious threats to public safety or to the safety of one or more persons in particular. In this case, the personal data may be processed by the receiving party only if that is absolutely necessary for the specific purpose for which the data have been supplied. Such data transfers shall be notified to the competent supervisory authority.

Justification

In view of the specific character of police and judicial work, it must be possible to transfer data to a third country in exceptional circumstances, on a case-by-case basis, even if the third country does not guarantee an adequate level of protection.

Amendment 40
Article 14 a (new)

Article 14a

Transmission to authorities other than competent authorities

Member States shall provide that personal data may be transmitted to authorities of a Member State other than competent authorities only in particular individual and well-founded cases and if all the following requirements are met:

(a) the transmission is provided for by a law clearly making it mandatory or authorising it, and

(b) the transmission is

- necessary for the specific purpose for which the data concerned were collected, transmitted or made available or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data

subject,

- necessary because the data concerned are indispensable to the authority to which the data are to be further transferred to enable it to fulfil its own lawful task and provided that the aim of the collection or processing to be carried out by that authority is not incompatible with the original processing, and the legal obligations of the competent authority which intends to transmit the data are not contrary to this

Justification

It is essential to provide for clear and strict provisions when data are transferred to non competent authorities.

Amendment 41
Article 14 b (new)

Article 14b

Transmission to private persons

Without prejudice to national rules of criminal procedure, Member States shall ensure that personal data are communicated to private persons in a Member State only if all the following conditions are met:

(a) their transmission is the subject of an obligation or of a clear legal authorisation;

(b) their transmission is necessary in order to attain the purpose for which the data in question were collected, transmitted or made available, or for the purposes of preventing or detecting criminal offences, or an investigation or prosecution pertaining thereto, or in order to avert threats to public safety or to a person, except where the need to protect the interests or fundamental rights of the data subject prevails over this type of consideration. The Member States shall provide that the competent authorities

may consult and process personal data controlled by private persons only on a case-by-case, in specific circumstances, for specific reasons and subject to judicial control in the Member States.

Justification

It is necessary to regulate strictly the communication of personal data to private persons.

Amendment 42
Article 14 c (new)

Article 14c

Processing of data by private persons when carrying out a public service remit

The national legislation of the Member States shall provide that, where private persons collect and process data as part of a public service remit, they are subject to requirements which are, at least, equivalent to or otherwise exceed those imposed on the competent authorities.

Justification

It is important to stipulate that, where data are processed by private persons, they are subject, at the minimum, to the same conditions as regards data security as apply to the competent public authorities.

Amendment 43
Article 16

The competent authority shall inform the subject of the collection of personal data of the fact that data relating to him are being processed, the categories of data involved and the purposes of the processing, unless the provision of such information proves, in the particular case, to be incompatible with the permissible purposes of the processing, or involves a disproportionate effort compared to the legitimate interests of the data subject.

The data subject shall be informed of the fact that personal data concerning him or her are being processed, the categories of data concerned, the identity of the controller and/or his or her representative, if any, the legal basis and the purposes of the processing, the existence of the right to access and rectify the data concerning him or her, unless the provision of such information proves impossible or incompatible with the purposes of the processing, or involves a

	disproportionate effort in relation to the data subject's interests, or where the data subject already has that information.

Justification

Members of the public have an inalienable right to be informed if their personal data are used. This is a fundamental principle of data protection which must be upheld (see Principle 7 - information to be given to the data subject).

Amendment 44
Article 17, paragraph 1, point (b a) (new)

	(ba) the purposes for which the data are processed and communicated;

Justification

Article 17 is incomplete, since access shall include also the purposes for which data are processed and communication in an intelligible form.

Amendment 45
Article 17, paragraph 2, point (a)

a) It would jeopardise ***the proper performance of the tasks of the competent authority;***	a) It would jeopardise ***an ongoing operation;***

Amendment 46
Article 17, paragraph 2, point (b)

(b) it would jeopardise public order or security or otherwise be detrimental to national interests;	***deleted***

Justification

Exceptions laid down by paragraph 2 - such as the case when access would "otherwise be detrimental to national interests" - are too broad and unforeseeable.

Amendment 47
Article 17, paragraph 2, point (c)

c) the data or the fact of their storage must	c) the data or the fact of their storage must

be kept secret pursuant to a legal provision or by reason of their nature***, in particular for the sake of the overriding interests of a third party;***	be kept secret pursuant to a legal provision or by reason of their nature;

Amendment 48
Article 18, paragraph 1

1. The data subject is entitled to expect the competent authority to fulfil its duties concerning the rectification, erasure or blocking of personal data which arise from this Framework Decision	1. The data subject is entitled to expect the competent authority to fulfil its duties concerning the rectification, erasure or blocking of personal data which arise from this Framework Decision. ***The data subject shall also be entitled to access and rectify his own data.***

Amendment 49
Article 20

Without prejudice to any administrative remedy for which provision may be made prior to referral to the judicial authority, the data subject must have the opportunity of seeking judicial remedy for any breach of the rights guaranteed to him by the applicable national law.	Without prejudice to any administrative remedy for which provision may be made prior to referral to the judicial authority, the data subject must have the opportunity of seeking judicial remedy for any breach of the rights guaranteed to him by the applicable national law, ***which shall be determined pursuant to Article 19 (1)***.

Amendment 50
Article 21

Persons who have access to personal data which fall within the scope of this Framework Directive may process such data only as members or on the instructions of the competent authority, unless there are legal obligations to do so. ***Persons*** called upon to work for a competent authority of a Member State shall be bound by all the data protection rules which apply to the competent authority in question.	***Duly authorised staff*** who have access to personal data which fall within the scope of this Framework Directive may process such data only as members or on the instructions of the competent authority, unless there are legal obligations to do so. ***Duly authorised staff*** called upon to work for a competent authority of a Member State shall be bound by all the data protection rules which apply to the competent authority in question.

Amendment 51
Article 22, paragraph 2, point (g)

g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems and when and by whom the data were input (input control);	g) ensure that it is subsequently possible to verify and establish which personal data have been input ***or processed*** into automated data processing systems and when and by whom the data were input ***or processed*** (input ***and processing*** control);

Amendment 52
Article 23, introductory part

Member States shall provide that the processing of personal data shall be subject to prior checking by the competent supervisory authority where:	Member States shall provide that the processing of personal data shall be subject to prior checking ***and authorisation by the competent judicial authority as prescribed by national law and*** by the competent supervisory authority where:

Amendment 53
Article 24

Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Framework Decision and shall in particular lay down effective, proportionate and dissuasive sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Framework Decision.	Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Framework Decision and shall in particular lay down effective, proportionate and dissuasive sanctions, ***including administrative and/or criminal penalties in accordance with national law*** to be imposed in case of infringement of the provisions adopted pursuant to this Framework Decision.

Amendment 54
Article 25, paragraph 1, point (c)

c) the power to engage in legal proceedings where the national provisions adopted pursuant to this Framework Decision have been infringed or to bring such	c) the power to ***initiate or otherwise*** engage in legal proceedings where the national provisions adopted pursuant to this Framework Decision have been infringed or

infringements to the attention of the judicial authorities. Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts	to bring such infringements to the attention of the judicial authorities. Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts

Amendment 55
Article 26, paragraph 1 a (new)

	1a. The joint supervisory authority shall gather the national supervisory authorities provided for in Article 25 and the European Data Protection Supervisor.

Justification

The joint supervisory authority established by this Framework Decision must bring together the national data protection authorities of each Member State and the European authority in this field.

Amendment 56
Article 26, paragraph 2

2. The ***composition,*** tasks and powers of the joint supervisory authority shall be laid down by ***Member States through a Council Decision*** under Article 34(2)(c) of the Treaty on European Union. The joint supervisory authority shall in particular monitor the proper use of data processing programs by which personal data are to be processed and advise the Commission and Member States on any proposed amendment of this Framework Decision, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences and on any other proposed measures affecting such rights and freedoms.	***3.*** The tasks and powers of the joint supervisory authority shall be laid down by ***the Council*** under Article 34(2)(c) of the Treaty on European Union ***not later than 12 months after the date of entry into force of this Framework Decision***. The joint supervisory authority shall in particular monitor the proper use of data processing programs by which personal data are to be processed and advise the Commission and Member States on any proposed amendment of this Framework Decision, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences and on any other proposed measures affecting such rights and freedoms.

Justification

To enable the joint authority to be operational as quickly as possible, the Council must define its remit and powers within a certain time limit.

Amendment 57
Article 27, paragraph 1

1. This Framework Decision is without prejudice to any obligations and commitments incumbent upon Member States or upon the European Union by virtue of bilateral and/or multilateral agreements with third States.	1. This Framework Decision is without prejudice to any ***pre-existing*** obligations and commitments incumbent upon Member States or upon the European Union by virtue of bilateral and/or multilateral agreements with third States.

Justification

It is important to make it clear that international agreements negotiated after the adoption of this Framework Decision will have to accord with it.

Amendment 58
Article 27, paragraph 1 a (new)

	1a. Any bilateral and/or multilateral agreement which enters into force after the date of entry into force of this Framework Decision shall comply with this Framework Decision;

Justification

It is important to make it clear that international agreements negotiated after the adoption of this Framework Decision will have to accord with it.

Amendment 59
Article 27 a (new)

	Article 27a
	Assessment and revision
	1. Not more than three years after the date of entry into force of this Framework Decision, the Commission shall submit to the European Parliament and the Council an assessment of the application of this

Framework Decision, accompanied by proposals for any amendments which are necessary in order to extend its scope pursuant to Article 1(6).

2. To this end, the Commission shall take account of the observations forwarded by the parliaments and governments of the Member States, the Article 29 working party, the European Data Protection Supervisor and the joint supervisory authority provided for in Article 26.

Justification

It is important to provide for machinery to assess the application of this Framework Decision and if appropriate the possibility of amending it on the basis of the recommendations of the competent authorities.

Amendment 60
Annex (new)

15 Principles on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

Principle 1

(Protection of rights and freedoms)

1. Personal data must be processed by ensuring a high level of protection of data subjects' rights, fundamental freedoms and dignity, including the right to personal data protection.

Principle 2

(Minimisation)

1. The use of personal data shall be configured by minimising their processing if the purposes sought can be achieved by using anonymous or non identifying information.

Principle 3

(Transparency)

1. The processing of personal data must be transparent under the terms set out in

the law.

2. The type of data and processing operations, the relevant retention period, and the identity of the controller and processor(s) must be specified and made available.

3. The results achieved by means of the various categories of processing performed should be publicised regularly in order to assess whether the processing is further helpful in concrete.

Principle 4

(Legitimacy of processing)

1. Personal data may only be processed if this is provided for by a law setting out that processing by the competent authorities is necessary in order for the said authorities to fulfil their legitimate obligations.

Principle 5

(Data quality)

1. Personal data must be:

-processed fairly and lawfully;

-collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

-adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

-accurate and, where necessary, kept up to date;

-kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and/or further processed, in particular where the data are available on line.

2. Personal data must be evaluated taking into account their degree of accuracy or reliability, their source, the categories of data subjects, the purposes for which they

are processed and the phase in which they are used. Every reasonable step should be taken to ensure that data which are inaccurate or incomplete are erased or rectified.

3. Data mining and any form of large-scale processing of massive quantities of personal data, in particular where related to non-suspects, including the transfer of such data to a different controller, shall only be permitted if carried out in compliance with the results of an examination performed by a supervisory authority either prior to the start thereof or in the context of preparation of a legislative measure.

4. Personal data must be processed by separating facts and objective evaluations from opinions or personal assessments, and the data related to prevention and prosecution of offences from data lawfully held for administrative purposes.

5. Appropriate checks prior and after an exchange of data must be established.

6. The controller shall take suitable measures in order to facilitate respect for the principles laid down herein, including by means of ad hoc software, as also related to the possible notification of rectification, erasure or blocking to third party recipients.

Principle 6

(Special categories of data)

1. The processing of personal data solely on the basis that they reveal racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, and the processing of personal data concerning health or sex life shall be prohibited. The processing of these data may only be carried out if absolutely necessary for the purpose of a particular inquiry.

2. Appropriate safeguards shall be

provided for by specific provisions, or on the basis of prior checking, in respect of processing operations that are likely to present specific risks to the rights and freedoms of data subjects, such as in particular the processing of DNA profiles, biometric data, data of non-suspects and the use of particular surveillance techniques or new technologies.

Principle 7

(Information to be given to the data subject)

1. The data subject shall be informed of the fact that personal data concerning him are being processed, the categories of data concerned, the identity of the controller and/or his representative, if any, the legal basis and the purposes of the processing, the existence of the right to access and rectify the data concerning him, unless the provision of such information proves impossible or incompatible with the purposes of the processing, or involves a disproportionate effort compared to data subject's interests, or where the data subject already has this information.

2. The provision of information to the data subject may be delayed to the extent this is necessary in order not to jeopardize the purposes for which the data were collected and/or further processed.

Principle 8

(Right of access to data and rectification)

1. The data subject shall have the right to obtain from the controller, without constraint at reasonable intervals and without excessive delay:

a. confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom data are disclosed,

b. communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

c. knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in principle 9;

2. The data subject shall have the right:

a. to rectification or, if appropriate, erasure of data that are processed in breach of these principles, in particular because of the incomplete or inaccurate nature of the data,

b. to have third parties to whom the data have been disclosed notified of any rectification or erasure carried out in compliance with (a), unless this proves impossible or involves a disproportionate effort.

3. The communication referred to in paragraph 1 may be refused or delayed if such a refusal or delay is necessary to:

a. protect security and public order or to prevent crime; or

b. the investigation, detection and prosecution of criminal offences; or

c. protect the rights and freedoms of third parties.

Principle 9

(Automated individual decisions)

1. Everyone has the right not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him.

2. Subject to other principles, a person may be subjected to a decision of the kind referred to herein if that decision is authorised by a law which also lays down appropriate measures to safeguard the

data subject's legitimate interests.

Principle 10

(Confidentiality and security of processing)

1. The controller and any person acting under the authority of the latter should not disclose or anyhow make available any personal data to which access is necessitated by virtue of their function, unless authorised or required to do so by law.

2. The controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss or unauthorised disclosure, alteration and access or all other unlawful forms of processing. These measures should be of a level appropriate to the risks arising from the processing and the nature of the data to be protected, by also considering the reliability and confidentiality of the data, and must be reviewed periodically.

Principle 11

(Communication of personal data)

1. The communication of data should only be permissible if there exists a legitimate interest for such communication within the framework of the legal powers of the competent authorities.

2. Data communicated in accordance with the principles set forth herein should only be used for the purposes for which they have been disclosed or, if provided for by the law or agreed upon by the competent authorities, where a concrete link exists with an ongoing investigation.

3. Communication to other public bodies or private parties should only be permissible if, in a particular case:

a. there exists a clear legal obligation or authorisation, or with the authorisation of

the supervisory authority, or if

b. these data are indispensable to the recipient to enable him to fulfil his own lawful task and provided that the aim of the collection or processing to be carried out by the recipient is not incompatible with the original processing, and the legal obligations of the communicating body are not contrary to this.

4. Furthermore, communication to other public bodies is exceptionally permissible if in a particular case:

a. the communication is undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent, or if

b. the communication is necessary so as to prevent a serious and imminent danger.

5. Communication of data to third countries or international bodies should be subject to the existence of an appropriate legal framework resulting from an examination performed prior to the start thereof by a supervisory authority or in the context of a legislative measure, providing in particular, that the request for such communication contains clear indications as to the body or person requesting them, the purpose, the proportionality and the security measures of the processing, and the adequate guarantees to ensure a mandatory framework about the use of data. Such guarantees should be assessed in general on the basis of a standard procedure by taking into account all the principles set out in this Annex.

Principle 12

(Notification and prior checking)

1. Member States shall identify the categories of permanent or ad hoc files likely to present specific risks to the rights and freedoms of data subjects, to be

notified to a supervisory authority or subject to a prior checking under the conditions and procedures to be specified by domestic law.

Principle 13

(Responsibility)

1. The controller is responsible for ensuring that the provisions set out in these principles are respected, in particular as for any activities performed by and/or committed to processors acting under his instructions.

Principle 14

(Judicial remedies and liability)

1. Every person has the right to a judicial legal remedy for any breach of the rights guaranteed to him by these principles.

2. The data subject has the right to compensation for any damage suffered by him because of the unlawful processing of personal data concerning him.

3. The controller may be exempted from his liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage

Principle 15

(Supervision)

1. Observance of the principles of personal data protection should be monitored and enforced by one or more public supervisory authorities. The supervisory authorities should in particular be endowed with powers of investigation and intervention allowing them in particular to instigate, as appropriate, the rectification or erasure of personal data whose processing does not comply with the principles established in this Annex. These authorities shall act in complete independence in exercising the

functions entrusted to them.

2. The supervisory authorities shall be consulted when drawing up legislative and administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data or otherwise having an impact on them.

3. The supervisory authorities shall be endowed with:

a. investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of their supervisory duties,

b. effective powers of intervention, such as, for example that of delivering opinions before processing operations are carried out, in accordance with principle 12, and of ordering erasure or destruction of data, of imposing a definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to the Parliament or other political institutions,

c. the power to engage in legal proceedings where the principles have been violated or to bring these violations to the attention of judicial authorities.

Decisions by the supervisory authorities which give rise to complaints may be appealed against through the courts.

4. Supervisory authorities shall hear and decide on claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in respect of the processing of personal data. The person concerned shall be informed of the outcome of the claim.

The supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by

any person when the principle 8.3 is applied. The person shall at any rate be informed that a check has taken place.

5. Supervisory authorities shall draw up a report on their activities at regular intervals. The report shall be made public.

Justification

The European Parliament has for several years been calling on the Council to adopt common principles relating to protection of data used for security purposes. The rapporteur endorses these 15 principles and calls on the other European institutions to follow suit.

EXPLANATORY STATEMENT

Background

In December 2005, at the time of the adoption of the Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services, the Council reaffirmed the commitment of several successive Presidencies to the swift adoption of a framework decision on the protection of personal data in the third pillar.

The European Parliament, aware of the urgency of the harmonisation of the rights of European citizens and protection of their privacy in connection with police and judicial cooperation, adopted its opinion on 14 June 2006, proposing a number of amendments to enhance the Commission proposal. In its legislative resolution adopted on 27 September 2006, Parliament called on the Council 'to consult Parliament again if it intends to amend the Commission proposal substantially'.

After deadlock had been reached within the Council on this framework decision, the European Parliament adopted, on 14 December 2006, a recommendation to the Council in which it stated that it was 'extremely concerned at the direction being taken by the debate in the Council, with Member States appearing to be moving towards a data protection agreement based on the lowest common denominator,' and feared, 'moreover, that the level of data protection will be lower than that provided by Directive 95/46/EC and Council of Europe Convention No 108 and that implementation of such an agreement might have a negative impact on the general principle of data protection in each Member State without establishing a satisfactory level of protection at European level'.

Renewed consultation of the European Parliament

I wish first of all to welcome the efforts made by the German Presidency, which have made it possible to overcome the deadlock within the Council over this framework decision. The revised proposal for a framework decision proposed by the Presidency has made it possible to reach political agreement, which should mean that it can be adopted swiftly. I also welcome the Council's appreciation of the need to keep the European Parliament fully involved in these negotiations by formally re-consulting it.

A framework decision on data protection in the third pillar is an indispensable instrument for the establishment of a genuine area of freedom, security and justice. The exchange of growing quantities of data, including personal data, in the fields covered by the third pillar must meet European Union requirements regarding the protection of fundamental rights and must comply with Articles 7 and 8 of the Charter of Fundamental Rights (respect for private life and protection of personal data). However, if we wish to make it possible to reinforce the principle of mutual confidence between the competent authorities and thereby contribute to better functioning of European police and judicial cooperation, the level of protection afforded by this framework decision must represent added value in relation to existing provisions, particularly the Council of Europe's Convention 108 and Recommendation 87.

The European Parliament has for some years been calling on the Council to adopt common principles relating to the protection of data used for security purposes. The existence of such principles would be useful not only to direct activities within the EU but also as a basis for negotiations with third countries, particularly the United States, and international organisations.

There has not been a satisfactory response to this suggestion, despite proposals put forward during the Italian and Greek Presidencies.

The problem was ultimately broached again under the German Presidency and during a trialogue between your rapporteur, Minister Schäuble and Commissioner Frattini on 28 March 2007. On that occasion the Commissioner gave me a draft text setting out 15 general principles which summarised the existing approach to protection of personal data processed in the framework of police and judicial cooperation in criminal matters, derived from the relevant international conventions and European law, which you will find attached.

As rapporteur, I am bound to welcome this initiative and the quality of the work submitted to me.

I endorse these 15 principles and I propose that they should serve as a background to our legislative work in this field and a basis for negotiations with third countries.

I consider, incidentally, that the other institutions should adopt formal positions on them, and I would like to propose that they be mentioned during the plenary debate, incorporated in the Plenary Minutes as an interinstitutional declaration and recalled in the legislative resolution stating the EP's opinion of the Council position in this report.

Substance of the new proposal for a framework decision

I welcome the fact that we have reached agreement on this text, which the Parliament has been calling for since the creation of the third pillar. However, I have on several occasions stressed that the necessary speed of the negotiations should not be allowed to detract from the quality of the framework decision and the level of protection of privacy for which it provides. This framework decision must afford a high level of data protection for citizens and added value in relation to the provisions in force in this field. Although it does not yet permit genuine harmonisation at this stage, the framework decision should on no account allow a level of protection less than that ensured by Convention 108.

In his third opinion on this proposal for a framework decision, the European Data Protection Supervisor stated that, as it stands, there is a risk that the text may reduce the level of protection enjoyed by citizens and fall short of the level guaranteed by Convention 108. He also underlined the fact that this lowest common denominator will not serve the creation of an area of freedom, security and justice, as the exchange of personal data by the competent authorities will be subject to different levels of protection.

I therefore propose a series of amendments to return to what European Parliament regarded as the main points when adopting its first report:

- scope
Although we may welcome the extension of the scope of this instrument to Europol and Eurojust, it has not been extended to data processing at national level. Only one recital (Recital 6a) alludes to this possibility. Yet this is absolutely necessary, for it is impossible to determine in advance whether or not data will be communicated to another Member State. In order not to apply different levels of data protection, the framework decision should be of wide scope, including processing of data at national level. Aware of the problems which this poses within the Council, I propose setting a time limit of three years, at the end of which the Commission should conduct an assessment and make proposals for extending the scope of the decision.

- subsequent processing of data
The principle of purpose is a fundamental principle of data protection. The processing of data for 'any other purpose' as referred to in Article 12(d) is disproportionate and does not respect this principle. I propose limiting any subsequent processing in accordance with the existing data protection rules. Incidentally, the concept of consent by the person concerned was inserted by the Council as a criterion where data are processed for purposes different from those for which they were collected. I do not believe that there can be any genuinely free consent in the fields of police and judicial cooperation, and this concept should therefore be deleted.

- transfer of data to the third country
In view of the current discussions concerning the exchange of data with third countries, particularly on Swift and the PNR Agreement, it is necessary to adopt at European level minimum standards of data protection for these exchanges. Efforts to control organised crime and international terrorism require an effective exchange of information with our partners in the world. Such an exchange will be efficient and useful only if we establish a high level of data protection. The text proposed by the Council no longer refers to the need to ensure an adequate level of data protection in exchanges with third countries in accordance with Article 2 of the Additional Protocol to Convention 108. I propose reinserting it so that the framework decision does not fall short of existing standards of data protection. I also propose that the joint supervisory authority created in the framework decision should be able to advise the Council, so as to ensure an appropriate level of transfer of data to a third country in the light of national law and international agreements.

- transfer of data to private persons and access to data relating to private persons
During the negotiation of the Directive on data retention, the Council gave a moral commitment to consider the issue of access to data stored by private persons in connection with a public-service remit and for security purposes. This no longer figures in the text submitted to us for renewed consultation. I propose therefore that we should reinstate Article 14b, which we adopted in our first report. It is also desirable to define clearly the conditions for transfer of personal data to private persons.

- clarifying the roles of the new joint supervisory authority and the national authorities
Directive 95/46/EC on the protection of data in the context of the first pillar already required the establishment of national data protection authorities. It seems to me that we should exploit the expertise of the existing authorities wherever possible. I therefore propose that the remit of

the existing authorities should be extended to the third pillar. The joint supervisory authority will be genuinely effective only if it combines the national authorities and the European Data Protection Supervisor, and I therefore propose stating its composition in the text of the framework decision.

- assessment and revision of the Framework Decision
As this framework decision does not yet permit genuine harmonisation of data protection in the third pillar, particularly if its scope is not extended, I propose inserting an assessment and revision clause so that the Commission can submit proposals for improving the framework decision after three years.

PROCEDURE

Title	Protection of personal data			
References	7315/2007 - C6-0115/2007 - 2005/0202(CNS)			
Date of Parliament's position - P number	27.9.2006		P6_TA(2006)0370	
Date of renewed consultation of Parliament	13.4.2007			
Committee responsible Date announced in plenary	LIBE 10.5.2007			
Committee(s) asked for opinion(s) Date announced in plenary	JURI 10.5.2007			
Not delivering opinion(s) Date of decision	JURI 21.5.2007			
Rapporteur(s) Date appointed	Martine Roure 26.9.2005			
Discussed in committee	11.4.2007	23.4.2007	8.5.2007	21.5.2007
Date adopted	21.5.2007			
Result of final vote	+: 30 –: 0 0: 2			
Members present for the final vote	Alexander Alvaro, Giusto Catania, Mladen Petrov Chervenyakov, Carlos Coelho, Fausto Correia, Panayiotis Demetriou, Agustín Díaz de Mera García Consuegra, Claudio Fava, Kinga Gál, Patrick Gaubert, Lilli Gruber, Jeanine Hennis-Plasschaert, Magda Kósáné Kovács, Wolfgang Kreissl-Dörfler, Barbara Kudrycka, Stavros Lambrinidis, Henrik Lax, Kartika Tamara Liotard, Sarah Ludford, Javier Moreno Sánchez, Martine Roure, Károly Ferenc Szabó, Søren Bo Søndergaard, Adina-Ioana Vălean, Ioannis Varvitsiotis, Manfred Weber, Tatjana Ždanoka			
Substitute(s) present for the final vote	Inés Ayala Sender, Simon Busuttil, Iratxe García Pérez, Sylvia-Yvonne Kaufmann, Bill Newton Dunn, Rainer Wieland			