EUROPEAN PARLIAMENT

2004 *2009*

Committee on Civil Liberties, Justice and Home Affairs

PROVISIONAL
2005/0202(CNS)

6.3.2006

*

DRAFT REPORT

on the proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

(COM(2005)0475 – C6-0436/2005 – 2005/0202(CNS))

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Martine Roure

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 5

EXPLANATORY STATEMENT.....39

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 co-operation in criminal matters (COM(2005)0475 – C6-0436/2005 – 2005/0202(CNS))

(Consultation procedure)

The European Parliament,

– having regard to the Commission proposal (COM(2005)0475)[1],

– having regard to Article 34(2)(b) of the EU Treaty,

– having regard to Article 39(1) of the EU Treaty, pursuant to which the Council consulted Parliament (C6-0436/2005),

– having regard to the Protocol integrating the Schengen acquis into the framework of the European Union, pursuant to which the Council consulted Parliament,

– having regard to the opinion of the Committee on Legal Affairs on the proposed legal basis,

– having regard to Rules 93 and 51 of its Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A6-0000/2006),

1. Approves the Commission proposal as amended;

2. Calls on the Commission to alter its proposal accordingly, pursuant to Article 250(2) of the EC Treaty;

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

4. Calls on the Council to consult Parliament again if it intends to amend the Commission proposal substantially;

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

Text proposed by the Commission	Amendments by Parliament

[1] OJ C ?, 1.3.2006, p. ?.

Amendment 1
Citation 1

Having regard to the Treaty on European Union, and in particular Article 30***, Article 31 and Article 34 (2)(b)*** thereof***,***	Having regard to the Treaty on European Union, and in particular Article 30***(1)(b) and Article 31(1)(c***) thereof,

Justification

It is necessary to be more precise about the legal basis. Article 30(1)(b) specifically refers to the exchange of information and data protection in the context of police cooperation. Article 31(1)(c) refers to improving judicial cooperation, including 'compatibility in rules applicable in the Member States'. Incidentally, these two articles constitute a legal basis such that the scope is not confined to data exchanged between the competent authorities of Member States but also covers internal situations.

Amendment 2
Citation 2 a (new)

	Having regard to the Opinion of the European Data Protection Supervisor,

Justification

It is essential to take account of the opinion of the European Data Protection Supervisor in drafting this framework decision.

Amendment 3
Recital 9

(9) Ensuring a high level of protection of the personal data of European ***citizens*** requires common provisions to determine the lawfulness and the quality of data processed by competent authorities in other Member States.	(9) Ensuring a high level of protection of the personal data of ***those residing in the*** European ***Union*** requires common provisions to determine the lawfulness and the quality of data processed by competent authorities in other Member States***. It also requires that personal data are collected and processed for legitimate and specific purposes. The data cannot be further processed in a way incompatible with***

	those purposes including in the framework of the increasing exchange of information between law enforcement and judicial authorities and in relation to the proposal on the interoperability of databases.

Justification

Everybody must be able to enjoy the benefit of data protection - not only European citizens. The purpose for which the data have been gathered must also be respected in connection with exchanges between police and judicial authorities.

Amendment 4
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 should benefit from an adequate level of protection. ***This Framework Decision should ensure that personal data received from third countries comply at least with international standards on the respect of human rights.***

Justification

Exchanges of data with third countries must respect two fundamental principles: they must ensure that the data can be transferred only to third countries which guarantee an appropriate standard of data protection and that data received from third countries respect fundamental rights.

Amendment 5
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. Furthermore, it is necessary that Member States provide for	(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 ***and by private parties processing personal data on behalf of competent authorities or in a public function,*** as well as judicial

criminal sanctions for particularly serious and intentionally committed infringements of data protection provisions.	remedies available for the data subject. Furthermore, it is necessary that Member States provide for criminal sanctions for particularly serious and intentionally committed infringements of data protection provisions.

Justification

It is important to state that where the data are managed by private parties, particularly in connection with public-private partnerships, they are subject, at the minimum, to the same data security conditions as laid down for the public competent authorities.

Amendment 6
Recital 20

(20) The present Framework Decision is without prejudice to the specific data protection provisions laid down in the relevant legal instruments relating to the processing and protection of personal data by Europol, Eurojust and the Customs Information System.	(20) The present Framework Decision is without prejudice to the specific data protection provisions laid down in the relevant legal instruments relating to the processing and protection of personal data by Europol, Eurojust and the Customs Information System. ***However, in the longer term, the rules on data protection applicable to Europol, Eurojust and Custom Information System should be made fully consistent with the present Framework Decision, with a view to enhancing consistency and effectiveness of the legal framework on data protection.***

Justification

The proposal provides for Europol, Eurojust and the customs information system to be excluded from its scope, as these have their own personal data protection systems. As the establishment of a European area of freedom, security and justice generates increased exchanges of personal data between competent authorities, including with Europol and Eurojust, it would be inconsistent to exclude them. In due course, therefore, it is necessary to provide for convergence between the data protection principles in this Framework Decision and the principles of Europol, Eurojust and the customs information system.

Amendment 7
Recital 22

(22) It is appropriate that this Framework Decision 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 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 the European Police Office Europol.***

Justification

It is appropriate to insert a reference to the VIS to ensure that this Framework Decision also applies to access to the visa information system by the forces of law and order.

Amendment 8
Article 3, paragraph 2 a (new)

	2a. This framework Decision shall not apply if specific legislation under Title VI of the Treaty on European Union explicitly stipulates that personal data shall be processed, accessed or transmitted only under more specific conditions or restrictions.

Justification

This Framework Decision should not preclude more specific legislation, particularly governing data processing.

Amendment 9

Article 4, paragraph 1, point (d)

(d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. Member States may provide for the processing of data to varying degrees of accuracy and reliability in which case they must provide that data are distinguished in accordance with their degree of accuracy and reliability, and in particular that data based on facts are distinguished from data based on opinions or personal assessments;	(d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. ***However,*** Member States may provide for the processing of data to varying degrees of accuracy and reliability in which case they must provide that data are distinguished in accordance with their degree of accuracy and reliability, and in particular that data based on facts are distinguished from data based on opinions or personal assessments; ***Member States shall provide that the quality of personal data is verified regularly. As far as possible, judicial decisions as well as decisions not to prosecute shall be indicated and data based on opinions or personal assessments checked at source and their degree of accuracy or reliability indicated. Member States shall, without prejudice to national criminal procedure, provide that personal data are marked on request of the data subject if their accuracy is denied by the data subject and if their accuracy or inaccuracy cannot be ascertained. Such mark shall only be deleted with the consent of the data subject or on the basis of a decision of the competent court or of the competent supervisory authority;***

Justification

This paragraph is repositioned from Article 9(6). These provisions should be moved from Chapter III to Chapter II so that they apply to all processing of data by the forces of law and order and not only to data exchanged between Member States.

Amendment 10
Article 4, paragraph 4

4. Member States shall provide that processing of personal data is only necessary if	***deleted***
- there are, based on established facts, reasonable grounds to believe that the personal data concerned would make possible, facilitate or accelerate the prevention, investigation, detection or prosecution of a criminal offence, and	
- there is no other means less affecting the data subject and	
- the processing of the data is not excessive in relation to the offence concerned	

Justification

This formulation does not respect the criteria established by the case law of the European Court of Human Rights relating to Article 8 of the European Convention on Human Rights. The case law provides that it is possible to impose restrictions on the right to private life only if that is necessary in a democratic society and not if it would facilitate or accelerate the work of police or judicial authorities. It is therefore necessary to replace it. The criterion of necessity and proportionality of data will be reformulated in Article 5.

Amendment 11
Article 4, paragraph 4 a (new)

	4a. Member States shall take into account the different categories of data and the different purposes for which they are collected with a view to lay down appropriate conditions for collection, time limits, further processing and transfer of the personal data concerned. Personal data related to non-suspects shall be processed only for the purpose for which they were collected, for a limited period of time, with adequate limitations in access and transmission.

Justification

The distinction between the various types of data made in paragraph 3 is very useful. It should be enhanced, devoting particular attention to data concerning non-suspects, to which specific protection measures must apply as regards the conditions for collecting data, the storage period and arrangements for access by the authorities.

Amendment 12
Article 4a, paragraph 1 (new)

Article 4a

Further processing of personal data

1. Member States shall provide that personal data are only further processed, in accordance with this Framework Decision, in particular its Articles 4, 5 and 6,

(a) for the specific purpose they were transmitted or made available or

(b) if strictly necessary, in a specific case, for the purpose of the prevention, investigation, detection or prosecution of criminal offences

(c) 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.

Justification

Further processing of data must be limited, and this principle must be laid down in Chapter II so that it applies to all data processing performed by the forces of law and order, and not only data exchanged with other Member States. Any further processing must comply with the principle of the purpose for which the data were gathered and must be considered case by case.

Amendment 13
Article 4a, paragraph 2 (new)

	2. The personal data concerned shall be further processed for the purposes referred to in paragraph 1 (c) of this article only with the prior consent of the authority that transmitted or made available the personal data and the Member States may, subject to adequate legal safeguards, adopt legislative measures to allow this further processing.

Justification

See the justification for the previous amendment.

Amendment 14
Article 5, paragraph 1

Member States shall provide that personal data may be processed by the competent authorities only if provided for by a law setting out that the processing is necessary for the fulfilment of the legitimate task of the authority concerned and for the purpose of the prevention, investigation, detection or prosecution of criminal offences.	***1.*** Member States shall provide that personal data may be processed by the competent authorities only if***:***
	(a) provided for by a law setting out that the processing is necessary for the fulfilment of the legitimate task of the authority concerned and for the purpose of the prevention, investigation, detection or prosecution of criminal offences. ***(b) the data subject has unambiguously given his consent, provided that the processing is carried out in the interest of the data subject; or*** ***(c) processing is necessary for compliance with a legal obligation to which the controller is subject.*** ***(d) processing is necessary in order to protect the vital interests of the data subject.***

Justification

The principles of proportionality and necessity should be inserted in Article 5 with reference to data. The processing of personal data should be considered necessary only where the competent authorities can clearly demonstrate the need for it and on condition that it is not possible to employ measures which respect privacy more.

Amendment 15
Article 5, paragraph 1 a (new)

1a. Member States shall provide that processing of personal data is only necessary if:

- competent authorities can demonstrate, based on established facts, a clear need to process the personal data concerned for the prevention, investigation, detection or prosecution of a criminal offence, and

- there is no other means less affecting the data subject and

- the processing of the data is not excessive in relation to the offence concerned.

Justification

The principles of purpose and proportionality should be inserted as criteria for establishing whether data processing is lawful.

Amendment 16
Article 6, paragraph 2, indent 1

- processing is provided for by a law and absolutely necessary for the fulfilment of the legitimate task of the authority concerned for the purpose of the prevention, investigation, detection or prosecution of criminal offences or if the data subject has given his or her explicit consent to the processing, and	- processing is provided for by a law and absolutely necessary for the fulfilment of the legitimate task of the authority concerned for the purpose of the prevention, investigation, detection or prosecution of criminal offences ***and limited to a particular inquiry*** or if the data subject has given his or her explicit consent to the processing, ***provided that the processing is carried out in the interest of the data subject, and the refusal to consent would not lead to negative consequences being imposed on the data;*** and

Justification

Processing of sensitive data based on the explicit consent of the person concerned should be authorised only to the extent that the processing is performed in the person's own interests. Moreover, denial of consent should not have any adverse consequences for the person concerned.

Amendment 17
Article 6, paragraph 2 a (new)

	2a. Member States shall implement special technical and organisational requirements for the processing of sensitive data.

Justification

Member States should establish specific technical measures to keep sensitive data secure .

Amendment 18
Article 6, paragraph 2 b (new)

2b. Member States shall provide for additional specific safeguards with regard to biometric data and DNA profiles, with a view to guarantee that:

- Biometric data and DNA profiles are used only on the basis of well established and interoperable technical standards

- The level of accuracy of biometric data and DNA profiles is carefully taken into account and may be challenged by the data subject through readily available means

- The respect of the dignity and integrity of persons is fully ensured.

Justification

Additional rules should be instituted to protect biometric data and DNA profiles. These data are particularly sensitive, but are sometimes used in connection with police and judicial cooperation.

Amendment 19
Article 7, paragraph 1

1. Member States shall provide that personal data shall be stored for no longer than necessary for the purpose for which it was collected, ***unless otherwise provided by national law***. Personal data of persons referred to in Article 4(3) last indent shall be stored for only as long as is absolutely necessary for the purpose for which it was collected.	1. Member States shall provide that personal data shall be stored for no longer than necessary for the purpose for which it was collected ***or further processed, in accordance with Article 4(1)(e) and Article 4a.*** Personal data of persons referred to in Article 4(3) last indent shall be stored for only as long as is absolutely necessary for the purpose for which it was collected.

Justification

The possibility of a general exemption, conditional solely on the requirement that national law should provide otherwise, from the guarantees provided for must be eliminated. This would jeopardise the harmonisation of criteria for data protection and is incompatible with the right to data protection.

Amendment 20
Article 7, paragraph 2

2. Member States shall provide for appropriate procedural and technical measures ensuring that time limits for the storage of personal data are observed. Compliance with such time limits shall be regularly reviewed.	2. Member States shall provide for appropriate procedural and technical measures ensuring that time limits for the storage of personal data are observed. ***These measures shall include automatic and regular deletion of personal data after a certain period of time.*** Compliance with such time limits shall be regularly reviewed.

Justification

The measures guaranteeing the storage period must provide for automatic deletion after a definite period.

Amendment 21
Article 8

Member States shall provide that personal data shall only be transmitted or made available to the competent authorities of other Member States if necessary for the fulfilment of a legitimate task of the transmitting or receiving authority and for the purpose of the prevention, investigation, detection or prosecution of criminal offences.	Member States shall provide that personal data ***collected and processed by the competent authorities*** shall only be transmitted or made available to the competent authorities of other Member States if necessary for the fulfilment of a legitimate task of the transmitting or receiving authority and for the purpose of the prevention, investigation, detection or prosecution of ***specific*** criminal offences.

Justification

Only data gathered by the competent authorities may be forwarded to the competent authorities. This will make it possible to limit access and transmission of data retained by private parties.

Amendment 22
Article 9, paragraph 6

6. Member States shall, without prejudice to national criminal procedure, provide that personal data are marked on request of the data subject if their accuracy is denied by the data subject and if their accuracy or inaccuracy cannot be ascertained. Such mark shall only be deleted with the consent of the data subject or on the basis of a decision of the competent court or of the competent supervisory authority.	***deleted***

Justification

These provisions should be moved from Chapter III to Chapter II, so that they apply to all data processing by the forces of law and order and not only to data exchanged between Member States.

Amendment 23
Article 9, paragraph 7, indent 3

- if these data are not or no longer necessary for the purpose for which they were transmitted or made available.	- ***and in any case*** if these data are not or no longer necessary for the purpose for which they were transmitted or made available.

Justification

The data must be systematically deleted if they are no longer needed for the purpose for which they were forwarded or made available.

Amendment 24
Article 9, paragraph 9 a (new)

	9a. Member States shall provide that the quality of personal data transmitted or made available by third countries shall be specifically assessed as soon as they are received and the degree of accuracy and reliability indicated.

Justification

It is necessary to check the quality of the data received from third countries in order to indicate their reliability, including as regards respect for fundamental rights.

Amendment 25
Article 10, paragraph 1

1. Member States shall provide that each automated transmission and reception of personal data, in particular by direct automated access, is logged in order to ensure the subsequent verification of the reasons for the transmission, the transmitted data, the time of transmission, the authorities involved and, as far as the receiving authority is concerned, the persons who have received the data and who have given rise to their reception.	1. Member States shall provide that each automated ***access,*** transmission and reception of personal data, in particular by direct automated access, is logged in order to ensure the subsequent verification of the reasons for the ***access and*** transmission, the transmitted ***or accessed*** data, the time of transmission ***or access***, the authorities involved and, as far as the receiving authority is concerned, the persons who have received the data and who have given rise to their reception.

Justification

It is also necessary to log access to data in order to ensure that all access to data is legitimate.

Amendment 26
Article 10, paragraph 2

2. Member States shall provide that each non automated transmission and reception of personal data is documented in order to ensure the subsequent verification of the reasons for the transmission, the transmitted data, the time of transmission,	2. Member States shall provide that each non automated ***access***, transmission and reception of personal data is documented in order to ensure the subsequent verification of the reasons for the ***access or*** transmission, the transmitted ***or accessed***

the authorities involved and, as far as the receiving authority is concerned, the persons who have received the data and who have given rise to their reception.	data, the time of transmission ***or access***, the authorities involved and, as far as the receiving authority is concerned, the persons who have received the data and who have given rise to their reception.

Justification

It is also necessary to log access to data in order to ensure that all access to data is legitimate.

Amendment 27
Article 10, paragraph 3

3. The authority that has logged or documented such information shall communicate it without delay ***to the competent supervisory*** authority ***on request of the latter***. The information shall only be used for the control of data protection and for ensuring proper data processing as well as data integrity and security.	3. The authority that has logged or documented such information shall ***keep it at disposal of the competent supervisory authority and*** communicate it without delay ***to the said*** authority. The information shall only be used for the control of data protection and for ensuring proper data processing as well as data integrity and security.

Justification

The log must be made available to the competent supervisory authority without its so requesting.

Amendment 28
Article 13, introductory part

Member States shall provide that personal data ***received from or made available by the competent authority of another Member State*** are ***further*** transmitted to authorities, other than competent authorities, of a Member State only in particular cases and if all of the following requirements are met:	Member States shall provide that personal data are transmitted to authorities, other than competent authorities, of a Member State only in particular ***individual and well-documented*** cases and if all of the following requirements are met:

Justification

This article must apply to all police and judicial data, even if they are not forwarded or made available by the competent authorities of another Member State.

Amendment 29
Article 13, point (b), subparagraph 1

necessary for the specific purpose the data concerned were transmitted or made available for 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 for the specific purpose the data concerned were ***collected,*** transmitted or made available for 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

Justification

The purpose for which the data have been collected must also be a criterion for forwarding them to authorities other than the competent authorities. This article, as amended, may apply to all police and judicial data, even if they are not forwarded or made available by the competent authorities of another Member State.

Amendment 30
Article 13, point (c)

(c) The competent authority of ***the*** Member State that has transmitted or made available the data concerned to the competent authority that intends to further ***transmit*** them has given its prior consent to their further transmission.	***Where personal data have been received from or made available by*** the competent authority of ***another*** Member State***, personal data shall not be further transmitted to authorities, other than competent authorities, of a Member State unless the Member State*** that has transmitted or made available the data concerned to the competent authority that intends to further ***transfer*** them has given its prior consent to their further transmission.

Justification

Any further processing of data must be authorised by the authority which has made them available and must comply with the rules regarding further processing (Article 4 a (new)).

Amendment 31
Article 14

Member States shall, without prejudice to national criminal procedural rules, provide that personal data ***received from or made available by the competent authority of another Member State*** can be further transmitted to ***private parties in a Member State*** only in particular cases and if all of the following requirements are met:	Member States shall, without prejudice to national criminal procedural rules, provide that personal data can be transmitted to private parties in a Member State only in particular cases and if all of the following requirements are met:
(a) the transmission is provided for by law clearly obliging or authorising it, and	(a) the transmission is provided for by law clearly obliging or authorising it, and
(b) the transmission is necessary for the purpose the data concerned were transmitted or made available for 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, and	(b) the transmission is necessary for the purpose the data concerned were ***collected,*** transmitted or made available for 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, and
(c) the competent authority of the Member State that has transmitted or made available the data concerned to the competent authority that intends to further transmit them has given its prior consent to their further transmission to private parties.	***Where personal data have been received from or made available by the competent authority of another Member State, personal data shall not be further transmitted to authorities, other than competent authorities, of a Member State unless the Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transmission.***

Justification

This article should apply to all data and not only data forwarded by another Member State. The purpose for which the data have been gathered must also be respected. Any further

transfer to private parties must be authorised by the Member State which has made the data available.

Amendment 32
Article 14 a (new)

Article 14a

Member States shall provide that competent authorities may access and process personal data controlled by private parties only on a case-by-case basis, under specified circumstances, for specified purposes, and under judicial control in the Member States.

Justification

Access by the competent authorities to data stored by private parties should be regulated, and should be possible only on a case-by-case basis and for established, justified reasons. Such access should require authorisation by court decision.

Amendment 33
Article 14 b (new)

Article 14b

Data processing by private parties in connection with public administration

Member States shall lay down in their national legislation that, where private parties collect and process data in connection with public administration, they are subject to obligations which are, at the minimum, equivalent to and otherwise exceed those imposed on the competent authorities.

Justification

Where private parties collect or process data in connection with public administration, measures supplementary to Directive 95/46/EC, to which they are subject, and superior to those imposed on the competent authorities, should apply to them.

Amendment 34
Article 15, paragraph 1

1. Member States shall provide that personal data ***received from or made available by the competent authority of another Member State*** are not further transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.	1. Member States shall provide that personal data are not transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.

Justification

This article should apply to all data and not only to those forwarded by another Member State.

Amendment 35
Article 15, paragraph 1, point (b)

(b) The transfer is necessary for the purpose the data concerned were transmitted or made available for 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.	(b) The transfer is necessary for the purpose ***for which*** the data concerned were ***collected or*** transmitted or made available for 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.

Justification

The purpose for which the data were collected must likewise be respected.

Amendment 36
Article 15, paragraph 1, point (c)

(c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.	***deleted***

Justification

This article should apply to all data and not only to those forwarded by another Member State. The question of further transfer is addressed in the new paragraph 4a.

Amendment 37
Article15, paragraph 1, subparagraph 1 a (new)

	Where personal data have been received from or made available by the competent authority of another Member State, personal data shall not be further transferred to competent authorities of third countries or to international bodies unless the Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.

Justification

See justification to previous amendment.

Amendment 38
Article 15, paragraph 3

3. The Member States and the Commission shall inform each other of cases where they consider that a third country or an international body does not ensure an adequate level of protection within the meaning of paragraph 2.	3. The Member States and the Commission shall inform each other ***and the European Parliament*** of cases where they consider that a third country or an international body does not insure an adequate level of protection within the meaning of paragraph 2.

Justification

The European Parliament should also be consulted when assessing the level of data protection ensured by third countries.

Amendment 39
Article 15, paragraph 4

4. Where***, under the procedure provided for in Article 16, it is established*** that a third country or international body does not ensure an adequate level of protection within the meaning of paragraph 2, Member States shall take the measures necessary to prevent any transfer of personal data to the third country or international body in question.	4. Where ***the Commission, following the consultation of the Council and the European Parliament, establishes*** that a third country or international body does not ensure and adequate level of protection within the meaning of paragraph 2, Member States shall take the measures necessary to prevent any transfer of personal data to the third country or international body in question.

Justification

The European Parliament should also be consulted when assessing the level of data protection ensured by third countries.

Amendment 40
Article 15, paragraph 5

5. ***In accordance with the procedure referred to in Article 16, it may be established*** that a third country or	5. ***The Commission, following the consultation of the Council and the European Parliament may establish*** that a

international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law ***or*** of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.	third country or international body ensures an adequate level or protection within the meaning of paragraph 2, by reason of its domestic law ***and*** of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.

Justification

The European Parliament should also be consulted when assessing the level of data protection ensured by third countries.

Amendment 41
Article 15, paragraph 6

6. Exceptionally, personal data ***received from the competent authority of another Member State*** may be ***further*** transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons.	6. Exceptionally, ***as a derogation from paragraph 1, point (d),*** personal data may be transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons***. In this case, personal data shall be processed by the receiving party only insofar as it is absolutely necessary for the specific purpose for which they were transmitted. These transfers shall be communicated to the competent Supervisory Authority.***

Justification

The conditions for the applicability of the exception provided for in paragraph 6, which permits the transfer of data to third countries which do not adequately protect data, should be clarified. This exception should make it possible to grant exemptions only from the criterion of 'adequate protection' and not from the other principles enshrined in this Framework Decision. Data transfers in accordance with this exception must satisfy appropriate conditions and be notified to the competent supervisory authority.

Amendment 42
Article 16

Article 16	***deleted***
Committee	
1. Where reference is made to this Article, the Commission shall be assisted by a Committee composed of the representatives of the Member States and chaired by the representative of the Commission.	
2. The Committee shall adopt its rules of procedure on a proposal made by the Chair on the basis of standard rules of procedure which have been published in the Official Journal of the European Union.	
3. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The Committee shall deliver its opinion on the draft within a time limit which the chairperson may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 205(2) of the Treaty establishing the European Community, in the case of decisions which the Council is required to adopt on a proposal from the Commission. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairperson shall not vote.	
4. The Commission shall adopt the measures envisaged if they are in accordance with the opinion of the Committee. If the measures envisaged are not in accordance with the opinion of the Committee, or if no opinion is delivered, the Commission shall, without delay, submit to the Council a proposal relating to the measures to be taken and shall inform the European Parliament thereof.	
5. The Council may act by qualified majority on the proposal, within two months from the date of referral to the	

Council.

If within that period, the Council has indicated by qualified majority that it opposes the proposal, the Commission shall re-examine it. It may submit an amended proposal to the Council, resubmit its proposal or present a legislative proposal. If on the expiry of that period the Council has neither adopted the proposed implementing act nor indicated its opposition to the proposal for implementing measures, the proposed implementing act shall be adopted by the Commission.

Justification

The commitology procedure does not apply to the third pillar.

Amendment 43
Article 18

Member States shall provide that the competent authority from or by whom personal data were received or made available will be informed ***on request*** about their further processing and the achieved results.	Member States shall provide that the competent authority from or by whom personal data were received or made available will be informed about their further processing and the achieved results.

Justification

The competent authorities from which the data have been received must always be informed of any further processing.

Amendment 44
Article 19, paragraph 1, point (c) indent 4 a (new)

- the time limits for storing the data

Justification

The person concerned must be informed of the period for which the data concerning him or her will be stored.

Amendment 45
Article 19, paragraph 2, introductory part, points (a) and (b)

2. The provision of the information laid down in paragraph 1 shall be ***refused or*** restricted only if necessary	2. The provision of the information laid down in paragraph 1 shall ***not*** be ***provided*** or restricted only if necessary
(a) to enable the controller to fulfil its lawful duties properly,	
(b) to avoid prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competent authorities,	(b) to avoid prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the ***controller and/or the*** competent authorities,

Justification

Satisfactory processing of data should not be a criterion for refusing to communicate to the person concerned the information concerning him/her. That would constitute too broad and too vague a withdrawal of the rights of the person concerned.

Amendment 46
Article 19, paragraph 4

4. The reasons for a refusal or restriction according to paragraph 2 shall not be given if their communication prejudices the purpose of the refusal. In such case the controller shall inform the data subject that he may appeal to the competent supervisory authority, without prejudice to any judicial remedy and without prejudice to national criminal procedure. If the data subject lodges an appeal to the supervisory authority, the latter shall examine the appeal. The supervisory authority shall, when investigating the appeal***, only inform him of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.***	4. The reasons for a refusal or restriction according to paragraph 2 shall not be given if their communication prejudices the purpose of the refusal. In such case the controller shall inform the data subject that he may appeal to the competent supervisory authority, without prejudice to any judicial remedy and without prejudice to national criminal procedure. If the data subject lodges an appeal to the supervisory authority, the latter shall examine the appeal***. The supervisory authority shall, when investigating the appeal, inform the data subject of its outcome.***

Justification

The person concerned must be informed of the outcome of his or her appeal in every case and not only if corrections have been made.

Amendment 47
Article 20, paragraph 1, introductory part

1. Where the data have not been obtained from the data subject or have been obtained from him without his knowledge or without his awareness that data are being collected concerning him, Member States shall provide that the controller or his representative must, at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, ***within a reasonable time after the*** data are first disclosed, provide the data subject with at least the following information free of cost, except where he already has it or the provision of the information proves impossible or would involve a disproportionate effort:	1. Where the data have not been obtained from the data subject or have been obtained from him without his knowledge or without his awareness that data are being collected concerning him, Member States shall provide that the controller or his representative must, at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, ***no later than the time when*** data are first disclosed, provide the data subject with at least the following information free of cost, except where he already has it or the provision of the information proves impossible or would involve a disproportionate effort:

Justification

The concept of a 'reasonable time' is open to interpretation. It should therefore be clearly stated that, where the data have not been collected from the person concerned, information is provided to that person 'no later than the time when data are first disclosed'.

Amendment 48
Article 20, paragraph 2, introductory part and point (a)

2. The information laid down in paragraph 1 shall not be provided if necessary	2. The information laid down in paragraph 1 shall not be provided ***only*** if necessary
(a) to enable the controller to fulfil its lawful duties properly,	

Justification

Satisfactory processing of data should not be a criterion for refusing to communicate to the person concerned the information concerning him/her. That would constitute too broad and too vague a withdrawal of the rights of the person concerned.

Amendment 49
Article 21, paragraph 1, point (c)

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

Justification

Notification to third parties of any rectification must be systematic.

Amendment 50
Article 21, paragraph 2, introductory part and point (a)

2. Any act the data subject is entitled to according to paragraph 1 shall be refused if necessary	2. Any act the data subject is entitled to according to paragraph 1 shall be refused ***only*** if necessary
(a) to enable the controller to fulfil its lawful duties properly,	

Justification

Satisfactory processing of data should not be a criterion for refusing to communicate to the person concerned the information concerning him/her. That would constitute too broad and too vague a withdrawal of the rights of the person concerned.

Amendment 51
Article 22 a (new)

	Article 22a
	Automated individual decisions
	1. Member States shall grant the right to every person not to be subject to a decision or action 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, such as his reliability, conduct, etc
	2. Subject to the other Articles of this Framework Decision, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision or action is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests, such as readily available means allowing him to be informed about the logic involved in the automatic processing of data concerning him, to put his point of view, unless this is incompatible with the purpose for which data are processed.

Justification

Practical experience shows that the forces of law and order increasingly use automated data processing, and this should therefore be addressed in this Framework Decision. Decisions based purely on automated processing must be subject to very strict conditions and protection measures where they have legal consequences for the person or where they have a considerable impact on a person. These decisions or actions must be permitted only if they are expressly provided for by law, and should be subject to appropriate measures to protect the interests of the person concerned.

Amendment 52
Article 24, paragraph 1, subparagraph 2

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. ***Measures shall be deemed necessary where the effort they involve is not disproportionate to the objective they are designed to achieve in terms of protection.***	Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Justification

Technical and organisational measures to secure personal data are always necessary and should not be conditional on the efforts to which they give rise.

Amendment 53
Article 24, paragraph 2, point (j a) (new)

	(ja) implement measures to systematically monitor and report on the effectiveness of these security measures (systematic self-auditing of security measures)

Justification

Automated data processing should be systematically monitored to ensure that it is efficient and secure.

Amendment 54
Article 25, paragraph 1, introductory part

1. Member States shall provide that every controller keeps a register of any processing operation or sets of such an operation intended to serve a single purpose or several related purposes. The information to be contained in the register shall include	1. Member States shall provide that every controller keeps a register of any ***access and*** processing operation or sets of such an operation intended to serve a single purpose or several related purposes. The information to be contained in the register shall include

Justification

The register should also record access to the data.

Amendment 55
Article 26, paragraph 3

3. ***Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.***	3. ***Supervisory authorities shall be consulted on the provisions relating to the protection of individuals' rights and freedom when drawing up legislative measures in relation to data processing.***

Justification

The supervisory authorities, not the Member States, are responsible for protecting the rights of individuals when drawing up legislative measures relating to data processing.

Amendment 56
Article 29, paragraph 2 a (new)

2a. The Member States shall ensure that offences committed by private parties gathering or processing personal data in connection with public administration which correspond to serious violations of the provisions adopted pursuant to this Framework Decision, particularly of its provisions on confidentiality and the security of data processing, render the offender liable to effective, proportionate and dissuasive penalties under the criminal law.

Justification

Where private parties gather and process the data in connection with public administration, they must be subject to penalties under the criminal law for any abuse of the data.

Amendment 57
Article 30, paragraph 4, subparagraph 1 a (new)

Each supervisory authority shall, in particular, hear claims for checks of the lawfulness of data processing lodged by any person. The person shall at any rate be informed that a check has taken place.

Justification

The supervisory authority must also be able to verify the legality of the processing of the data and inform the person concerned about it.

Amendment 58
Article 31, paragraph 2, subparagraph 1

Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative.	Each member of the Working Party shall be designated by the institution, authority or authorities which he represents***, in accordance with the existing national rules regulating the representation.*** Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative.

Justification

The attendance of the chairperson of the Article 29 working party at the meetings of the new working party set up by this Framework Decision will make it possible to promote communication and exchanges between these two working parties.

Amendment 59
Article 31, paragraph 2, subparagraph 2 a (new)

	The chairperson of the Working Party set up by Article 29 of Directive 95/46/EC shall participate or be represented in the meetings of the Working Party.

Justification

The attendance of the chairperson of the Article 29 working party at the meetings of the new working party set up by this Framework Decision will make it possible to promote communication and exchanges between these two working parties.

Amendment 60
Article 31, paragraph 3

3. The Working Party shall take its decisions by a simple majority of the representatives of the supervisory authorities of the Member States.	3. The Working Party shall take its decisions by a simple majority of the representatives of the supervisory authorities of the Member States ***and the***

European Data Protection Supervisor.

Justification

The European Data Protection Supervisor will ensure consistency with the first-pillar Directives.

Amendment 61
Article 34 a (new)

Article 34a

Relation to Europol, Eurojust and Custom Information System

1. Not later than two years from the date referred to in Article 35(1), the Commission shall submit proposals with a view to making the rules on data protection applicable to Europol, Eurojust and the Custom Information System fully consistent with the present Framework Decision.

Justification

The proposal provides for the exclusion from its scope of Europol, Eurojust and the customs information system, as these have their own personal data protection systems. As the establishment of a European area of freedom, security and justice generates increased exchanges of personal data between competent authorities, including with Europol and Eurojust, it would be inconsistent to exclude them. In due course, therefore, it is necessary to provide for convergence between the data protection principles in this Framework Decision and the principles of Europol, Eurojust and the customs information system.

EXPLANATORY STATEMENT

Since the creation of the third pillar, the European Parliament has been calling for standards on data protection in the context of judicial and police cooperation which are comparable to the standards in force in Community law. These standards should replace the principles currently embodied in Council of Europe Convention 108 and Recommendation 87. We therefore welcome this Commission proposal responding to Parliament's request.

This instrument is necessary for two main reasons:

– the establishment of a European area of freedom, security and justice has led to the exchange of a growing quantity of data, including personal data, in the areas covered by the third pillar. This increased exchange must be subject to the European Union's requirements as regards 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);

– better data protection would reinforce the principle of mutual confidence between competent authorities and thus contribute to more effective European cooperation on police and judicial matters.

The draft framework decision[1] presented by the Commission is all the more important in the context of the recent adoption of the draft directive on the retention of data processed in connection with the provision of public electronic communication services[2]. When it adopted the latter, the European Parliament added an explicit request for this framework decision:

'… Considers that, concerning access to data, the present directive constitutes just a necessary first step and calls on the Council for loyal cooperation for the swift adoption of appropriate guarantees in the context of the framework decision on data protection and data treatment in judicial and police co-operation in criminal matters'.

Relationship with other proposals (SIS II, VIS, principle of availability)

The proposal for a framework decision on data protection under the third pillar is linked to several proposals currently being scrutinised by Parliament, notably those on VIS[3], SIS II[4], the principle of availability[5] and interoperability of European data in the area of JHA[6], since these provide for databases or measures facilitating access by the competent authorities to personal data.

The Community proposals on VIS and SIS II, for example, also include a proposal under the third pillar to provide for data access and use by the police and judicial authorities. These proposals should include clear references to the principles of personal data protection set out in the present framework decision.

It is for this reason that the framework decision should be adopted at the same time as the proposals on SIS II.

The proposal for a framework decision also refers to the availability principle, the aim of

which is that the information needed to combat crime should cross internal borders unimpeded via direct on-line access for the Member States' law-enforcement services and Europol agents.

Two obstacles to availability of data are noted, however:

- differing levels of protection are an impediment to the exchange of confidential information,
- there are no common rules on monitoring the legality of the use made of information obtained from another Member State, and the possibilities for tracing the source and the purpose of the information are limited.

The adoption of common rules on protection of data where the latter is intended for security purposes is also, therefore, a sine qua non for establishing the availability principle. Of course, while the success of the availability principle is dependent upon adoption of the present framework decision, the latter should nevertheless be adopted without prejudging the outcome of the discussions on the availability principle.

We must ensure that there is coherence and uniformity in the principles of data protection in the European Union, inter alia between the first and third pillars. The principles set out in Directive 95/46/EC should constitute the core of European law on this subject and lay down the general principles of data protection.

As rapporteur, I would like to incorporate in the third pillar to as great an extent as possible the principles of data protection established by the Community directives, in order to guarantee the same level of protection, while taking account also of the special nature of police and judicial work. The rules contained in Directive 95/46/EC must, for example, be supplemented with rules in the area of judicial and police cooperation on criminal matters, while maintaining coherence with the general principles established by Community law.

In order to do this, it is essential that the common rules on data protection should apply to all data in the police and judicial areas, and not be limited to cross-border exchanges between Member States. I would like to support a broad field of application for the framework decision, so that the European rules will also be applied to processing data within the Member States.

Europol, Eurojust and the customs information system are excluded from the proposals for a framework decision because they have their own data protection rules. In order to ensure that there is coherence among the data protection rules, including those applying to the agencies and bodies set up by the Union, I wish to encourage convergence between the specific rules of those bodies and this framework decision.

I therefore propose adding a new article in the 'Final Provisions' calling on the Commission to submit a proposal within two years with a view to making the rules on data protection applicable to Europol, Eurojust and the customs information system.

Data collection must be limited to specific purposes and must be carried out in accordance with the principles of proportionality and necessity. For example, any subsequent processing of the data must comply with precise rules, and subsequent transfer for purposes other than those for which the data were collected must be strictly limited. I propose drafting a new article defining subsequent treatment. I also propose inserting in Article 7 a measure

providing for automatic deletion of personal data after a fixed period.

The different categories of data (relating to suspects, convicted people, victims, witnesses etc.) are treated differently, with specific safeguards. I therefore propose adding a paragraph to Article 4 stipulating that data relating to people who are not under suspicion should be used solely for the purposes for which they were collected.

Additional safeguards must be added to Article 6 to cover DNA and biometric data in order to guarantee the safety and quality of the data and compliance with fundamental rights in using them.

This instrument enables us to define access to data by the competent authorities. In it we must define access to data kept by private parties, as is done in the directive on data retention. I therefore propose that a new article be inserted after Article 14 specifying that access to these data is to be granted on a case-by-case basis, for a specific purpose and under the judicial control of the Member States.

As regards the role of private parties in the management and processing of data for security purposes within a public service, I propose that these activities be made subject to very strict conditions laid down in national law and subject to penal sanctions.

Transfer of data to third-country authorities cannot be completely excluded in the context of international cooperation on fighting large-scale organised crime. It must, however, be strictly supervised. Firstly, data will be transferred to a third country only if the latter guarantees an adequate level of protection for the data. Secondly, the quality of data received from a third country will be assessed, inter alia in the light of fundamental rights. No data obtained by torture, for example, will be used by the European authorities.

We must add the questions of access and of automated decisions to the framework decision, as is done in other data protection instruments. The growing number of European databases means that authorities in one Member State can automatically access data collected by those in another. But this automatic access must not jeopardise fundamental rights. I therefore propose inserting a new article stipulating that a decision having an effect on an individual may not be taken on the sole basis of automated processing of data pertaining to them. In addition, I would like to use amendments to clarify that access to and use of these databases by the competent law-enforcement authorities must be governed by the principles and provisions of the framework decision.

---

[1] Proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters {SEC(2005) 1241} COM/2005/0475 final – CNS 2005/0202.
[2] See the text adopted by the EP on 14/12/05 (doc. P6_TA-PROV(2005)0512).
[3] Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas {SEC(2004) 1628} COM/2004/0835 final - COD 2004/0287.
[4] Regulation of the European Parliament and of the Council on the establishment, operation and use of the second-generation Schengen information system (SIS II) COM/2005/0236 final - COD 2005/0106.
Proposal for a Regulation of the European Parliament and of the Council regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates COM/2005/0237 final - COD 2005/0010.

Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II) COM/2005/0230 final - CNS 2005/0103.

[5] Proposal for a Council Framework Decision on the exchange of information under the principle of availability {SEC(2005) 1270} COM/2005/0490 final - CNS 2005/0207.

[6] Communication from the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs COM(2005)0597 final.