Procedure file

Basic information

CNS - Consultation procedure JHA act	2005/0202(CNS)	Procedure completed

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

Repealed by 2012/0010(COD)

Subject
1.20.09 Protection of privacy and data protection
7.30.05 Police cooperation
7.30.20 Action to combat terrorism
7.40.04 Judicial cooperation in criminal matters

Key players

European Parliament	Committee responsible	Rapporteur	Appointed
	LIBE Civil Liberties, Justice and Home Affairs		11/02/2008
		PSE ROURE Martine	
	Former committee responsible		
	LIBE Civil Liberties, Justice and Home Affairs		26/09/2005
		PSE ROURE Martine	
	LIBE Civil Liberties, Justice and Home Affairs		26/09/2005
		PSE ROURE Martine	
	Committee for opinion	Rapporteur for opinion	Appointed
	JURI Legal Affairs	The committee decided not to give an opinion.	
	Former committee for opinion		
	JURI Legal Affairs	The committee decided not to give an opinion.	
	Former committee for opinion on the legal basis		
	JURI Legal Affairs		12/12/2005
		ALDE WALLIS Diana	
Council of the European Union	Council configuration	Meeting	Date
	Justice and Home Affairs (JHA)	2908	27/11/2008
	Justice and Home Affairs (JHA)	2827	08/11/2007
	Justice and Home Affairs (JHA)	2818	18/09/2007
	Justice and Home Affairs (JHA)	2807	12/06/2007
	Justice and Home Affairs (JHA)	2768	04/12/2006
	Justice and Home Affairs (JHA)	2725	27/04/2006
European Commission	Commission DG	Commissioner	
	Justice and Consumers	BARROT Jacques	

Key events

	Legislative proposal published		Summary

04/10/2005		COM(2005)0475	
19/01/2006	Committee referral announced in Parliament		
27/04/2006	Debate in Council	2725	Summary
15/05/2006	Vote in committee		Summary
18/05/2006	Committee report tabled for plenary, 1st reading/single reading	A6-0192/2006	
13/06/2006	Debate in Parliament		
14/06/2006	Results of vote in Parliament		
14/06/2006	Decision by Parliament	T6-0258/2006	Summary
27/09/2006	Decision by Parliament	T6-0370/2006	Summary
04/12/2006	Debate in Council	2768	Summary
13/03/2007	Amended legislative proposal for reconsultation published	07315/2007	Summary
13/04/2007	Formal reconsultation of Parliament		
21/05/2007	Vote in committee		Summary
24/05/2007	Committee report tabled for plenary, reconsultation	A6-0205/2007	
06/06/2007	Debate in Parliament		
07/06/2007	Decision by Parliament	T6-0230/2007	Summary
12/06/2007	Resolution/conclusions adopted by Council		Summary
18/09/2007	Debate in Council	2818	Summary
08/11/2007	Debate in Council	2827	Summary
11/12/2007	Amended legislative proposal for reconsultation published	16069/2007	Summary
08/01/2008	Formal reconsultation of Parliament		
15/07/2008	Vote in committee		Summary
23/07/2008	Committee report tabled for plenary, reconsultation	A6-0322/2008	
23/09/2008	Debate in Parliament		
23/09/2008	Decision by Parliament	T6-0436/2008	Summary
27/11/2008	Act adopted by Council after consultation of Parliament		
27/11/2008	End of procedure in Parliament		
30/12/2008	Final act published in Official Journal		

Technical information

Procedure reference	2005/0202(CNS)

Procedure type	CNS - Consultation procedure
Procedure subtype	Legislation
Legislative instrument	JHA act
	Repealed by 2012/0010(COD)
Legal basis	Treaty on the European Union (after Amsterdam) M 030; Treaty on the European Union (after Amsterdam) M 031; Treaty on the European Union (after Amsterdam) M 034-p2b
Stage reached in procedure	Procedure completed
Committee dossier	LIBE/6/30877; LIBE/6/49216; LIBE/6/58016

Documentation gateway

Legislative proposal		COM(2005)0475	04/10/2005	EC	Summary
Document attached to the procedure		SEC(2005)1241	04/10/2005	EC	Summary
For information		52006XX0225(01) OJ C 047 25.02.2006, p. 0027-0047	19/12/2005	OS	
Committee draft report		PE370.250	06/03/2006	EP	
Amendments tabled in committee		PE372.160	25/04/2006	EP	
Committee report tabled for plenary, 1st reading/single reading		A6-0192/2006	18/05/2006	EP	
Committee opinion	JURI	PE374.335	01/06/2006	EP	
Text adopted by Parliament, partial vote at 1st reading/single reading		T6-0258/2006	14/06/2006	EP	Summary
Text adopted by Parliament, 1st reading/single reading		T6-0370/2006	27/09/2006	EP	Summary
Commission response to text adopted in plenary		SP(2006)4772	19/10/2006	EC	
Document attached to the procedure		N6-0005/2007 OJ C 091 26.04.2007, p. 0009	29/11/2006	EDPS	Summary
Amended legislative proposal for reconsultation		07315/2007	13/03/2007	CSL	Summary
Document attached to the procedure		N6-0015/2007 OJ C 139 23.06.2007, p. 0001	27/04/2007	EDPS	Summary
Committee draft report		PE388.564	04/05/2007	EP	
Amendments tabled in committee		PE388.613	14/05/2007	EP	
Committee final report tabled for plenary, reconsultation		A6-0205/2007	24/05/2007	EP	
Text adopted by Parliament after reconsultation		T6-0230/2007	07/06/2007	EP	Summary
Amended legislative proposal for reconsultation		16069/2007	11/12/2007	CSL	Summary
Committee draft report		PE402.702	10/03/2008	EP	
Amendments tabled in committee		PE406.124	16/05/2008	EP	

Committee final report tabled for plenary, reconsultation		A6-0322/2008	23/07/2008	EP	
Text adopted by Parliament after reconsultation		T6-0436/2008	23/09/2008	EP	Summary
Follow-up document		COM(2012)0012	25/01/2012	EC	Summary
Follow-up document		SEC(2012)0075	25/01/2012	EC	

Additional information

European Commission	EUR-Lex

Final act

Decision 2008/977
OJ L 350 30.12.2008, p. 0060 Summary

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

PURPOSE: to determine common standards to ensure the protection of individuals with regard to the processing of personal data.

PROPOSED ACT : Council Framework Decision

CONTENT: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data contains fundamental rules on the lawfulness of the processing of personal data as well as on the rights of the data subject. It includes provisions concerning judicial remedies, liability and sanctions, the transfer of personal data to third countries, codes of conduct, specific supervisory authorities and a working party and finally community implementing rules. However, the Directive does not apply to activities that fall outside the scope of Community law such as those provided for by Title VI of the Treaty on European Union (TEU). Accordingly Member States are allowed to decide themselves on appropriate standards for data processing and protection. In the context of Title VI TEU the protection of personal data is set out in different specific instruments.

This Framework Decision ensures the protection of personal data processed in the framework of police and judicial co-operation in criminal matters between the Member States of the European Union (TEU, Title VI). It aims at improving this cooperation, in particular regarding preventing and combating terrorism, and with the strict observance of key conditions in the area of data protection. It ensures that fundamental rights, with special attention to the right to privacy and to the protection of personal data, will be respected throughout the EU, in particular, in view of the implementation of the principle of availability. It also ensures that the exchange of relevant information between the Member States will not be hampered by different levels of data protection in the Member States.

The proposed Framework Decision includes general rules on the lawfulness of:

-processing of personal data;

-provisions concerning specific forms of processing (transmission and making available of personal data to the competent authorities of other Member States,

-further processing, in particular further transmission, of data received from or made available by the competent authorities of other Member States);

-rights of the data subject;

-confidentiality and security of processing;

-judicial remedies;

-liability;

-sanctions;

-supervisory authorities;

-a working party on the protection of individuals with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences.

Particular attention is to be paid to the principle that personal data are only transferred to those third countries and international bodies that ensure an adequate level of protection. The Framework Decision provides for a mechanism aiming at EU wide compliance with this principle.

This Framework Decision is based on Articles 30, 31 and 34 (2) (b) of the TEU.

On the matter of the principle of availability, the Commission takes the position that the implementation of the principle of availability will further develop and fundamentally change the quality and intensity of the exchange of information between the Member States. Such development will greatly affect personal data and the right to data protection. It needs to be appropriately counterbalanced. Recent initiatives aiming at direct

automated access, at least, on a hit/no hit basis are likely to increase the risk of exchanging illegitimate, inaccurate or non up-dated data and have to be taken into account. These initiatives imply that the data controller will no longer be able to verify in each individual case the legitimacy of a transmission and the accuracy of the data concerned. Consequently, this has to be accompanied by strict obligations to constantly ensure and verify the quality of data to which direct automated access is granted. Clear rules should be established for the protection of personal data that shall be or have been made available to competent authorities of other Member States. This implies a system ensuring the quality of processing of the data concerned. Such a system must include provisions laying down appropriate rights of the data subject and powers of the supervisory authorities as exercising those rights and powers is likely to contribute to the quality of the data concerned.

FINANCIAL IMPLICATIONS: The implementation of the proposed Framework Decision would entail only low additional administrative expenditure, to be charged to the budget of the EC, for meetings of and the secretarial services for the committee and the advisory body to be established according to Articles 16 and 31.

Period of application: starting 2006

Overall financial impact of human resources and other administrative expenditure: Total EUR 2,334 million over 5 years

Total Staff: 1.75

Overall financial impact of human resources: total EUR 189.000 per year

Other administrative expenditure deriving from the action: EUR 200.000 per year.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

COMMISSION?S IMPACT ASSESSMENT

For further information concerning the background to this issue, please refer to the summary of the Commission?s initialproposal 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*.

1- POLICY OPTIONS AND IMPACTS

The Commission considered six policy options.

1.1- Option 1 - No legislative initiative: The option of rejecting any legislative initiative would mean recourse to existing legal instruments, in particular Directive 95/46/EC and the Data Protection Convention of the Council of Europe. However, Directive 95/46/EC does not apply to the processing of personal data in the third pillar. Even the disappearance of the pillar architecture would not automatically result in the application of the Directive. Its Art 3 does not only clearly say that it shall not apply to processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union (TEU). It also explicitly excludes the applicability of the Directive in any case for processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

1.2- Option 2 - Application of Directive 95/46/EC: This would provide for the applicability of Directive 95/46/EC to data processing for the purpose of preventing and combating crime. This option is very close to the first one. Practically, it means transposing the provisions of the Directive (first pillar instrument) into a Framework Decision (third pillar instrument) without any or only slight modifications. However, most Member States also apply the Directive, irrespective of its Art 3, to data processing for the purpose of preventing and combating crime. However, Member States benefit from wide exceptions provided for by Art 13 of the Directive and thus have considerable discretion.

1.3- Option 3 - Legislative initiative once the modalities for the exchange of information under the principle of availability have been defined: The Commission also considered submitting, as a first step, a proposal defining the modalities of exchanging information under the principle of availability and developing appropriate data protection rules as a second step. In principle, it is possible to firstly determine the right modalities for the various types of information and to subsequently define the necessary supplementary rules for data processing and protection. Such approach stresses that data protection provisions can only be developed in view of a very specific purpose, a specific modality of the exchange of information and of a specific type of information.

On the other hand, this approach holds the risk of achieving agreement on (technical) modalities for the exchange of specific types of information (e.g. DNA, fingerprints) without reaching consensus on sufficient supplementary provisions on data processing and data protection. The right to data protection might be at risk in this case.

1.4- Option 4 - Specific provisions in a legal instrument on the exchange of information under the principle of availability: a set of provisions on data processing and protection to be included in a legal instrument on the exchange of information under the principle of availability. Option 4 could be based on the reasons supporting option 3 while avoiding possible disadvantages. A closer link between provisions defining the modalities of exchanging information under the principle of availability and appropriate provisions on data processing and protection could possibly be established. Both types of provisions would be negotiated and adopted by the Council at the same time. Finally, a well balanced chapter on data processing and protection within a legal act on the exchange of information under the principle of availability could probably foster police and judicial cooperation in criminal matters as well as promote proper respect for fundamental rights. On the other hand, option 4 would mean missing an opportunity to provide for a more coherent and consistent legal regime of the Union for data processing and protection. Such a regime could, in the long term, be based on a legal instrument providing for general rules in the area of data processing and protection.

1.5- Option 5 - Framework Decision on common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the TEU:

The fifth option is a Framework Decision setting out common standards for the processing and protection of personal data in the course of activities provided for by Title VI of the TEU. Contrary to Directive 95/46/EC and the instruments adopted within the Council of Europe, a

Framework Decision would provide for a complete system of legally binding provisions applicable to the direct exchange of information in the context of police and judicial cooperation in criminal matters while avoiding the weaker points of options 1 to 4. A framework decision setting out general rules for data processing and data protection would not only confirm the fundamental principles already established for the Community and by the Council of Europe but also provide for legally binding rules for all those questions that the various possible modalities of the exchange of information under the principle of availability have in common: not only principles relating to data quality but also more targeted rules for the criteria making data processing legitimate; obligations of the competent authorities when exchanging personal data; rights of the data subject, role of supervisory authorities, advisory body at EU level. This option would cover not only the principle of availability but more specific forms of police co-operation and exchange of information, such as the second generation of the SIS, the so-called ?SIS II?. However, a framework decision setting up common standards would not exclude the necessity of more specific rules where necessary.

1.6- Option 6 - Legislative initiative involving all existing EU information systems or bodies (Europol, Eurojust): The sixth option is a legislative initiative that aims at harmonising the rules for the processing and protection of personal data exchanged through central information systems and bodies (Europol, Eurojust) established at EU level, as well as for the direct exchange between the Member States. This option is the most far reaching one. It avoids the weakness of options 1 to 5 while providing for a high level of harmonisation and simplification regarding data processing and protection under Title VI of the TEU. In principle, this option is the most preferable with regard to the consistency and coherence of the Union?s policy on data processing and protection, but, as pointed out for option 5, more specific rules would have to be maintained or be set up, where necessary. Secondly, the option would require a comprehensive legislative package containing not only a framework decision setting up general rules for the processing and protection of personal data that are exchanged directly between the Member States but also modifications of the exchange of information through existing EU information systems or bodies. This would go beyond what seems to be immediately necessary in view of the principle of availability. It would require much more consultations and might be confronted with objections from the bodies concerned.

CONCLUSION: While further harmonisation including all information systems and bodies established at EU level is useful, it is less urgent than the rapid introduction of the principle of availability. The latter can be accompanied by an instrument on data processing and protection, which could then serve as the basis for further harmonisation. Such a two step approach would address the short term necessities as well as, in the long term, further harmonisation of the legislation on data processing and data protection under Title VI TEU. Therefore, the Commission recommends option 5.

IMPACT

Option 5 would provide for targeted rules on data processing and data protection for the exchange of information for the purpose of preventing and combating crime in the course of activities provided by Title VI of the TEU. It can ensure an appropriate data protection regime and avoid the disadvantages of options 1, 2 and 3.

A positive impact can also be expected on the respect of fundamental rights. Appropriate and targeted rules of the data protection regime would ensure that the data subject is generally well protected against unlawful processing of personal data. A comprehensive framework decision can be expected to have a more positive impact on the consistency of the Union?s policy on data protection.

Option 5 would not only cover the exchange of information under the principle of availability but also more specific forms of police co-operation and exchange of information, such as the second generation of the SIS, the so-called ?SIS II?. It could therefore be considered at least as a first step towards a less difficult and more transparent legal regime on data protection under Title VI TEU. Moreover, a framework decision could follow as far as possible the example of Directive 95/46/EC and contribute to a more consistent data protection policy ensuring a high level of data protection in both the first and the third pillar. Option 5 is unlikely to result in considerable additional costs. In general, Member States are likely to adapt their legislation. New bodies or systems are most probably not necessary. An advisory body for data protection issues related to police and judicial cooperation in criminal matters including secretarial services would generate costs for a number of meetings per year.

2- FOLLOW-UP

The proposed option shall be evaluated in accordance with the usual procedures under this Title VI. Member States shall transmit to the General Secretariat of the Council and to the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Framework Decision. On the basis of this information and a written report from the Commission, the Council shall assess before December 2007 the extent to which Member States have taken the measures necessary to comply with this Framework Decision.

Furthermore, a working party shall be established according to the Framework Decision. The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission. The European Data Protection Supervisor and the chairpersons of the joint supervisory bodies set up under Title VI of the Treaty on European Union shall be entitled to participate or to be represented in meetings of the Working Party.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The Austrian Presidency informed the Council of the state of play of discussion on this draft Framework Decision on the protection of personal data. The following issues have been debated:

- whether both police and judicial cooperation should be included in the scope of the draft Framework Decision;
- the question of extending the scope to law enforcement agencies other than the police;
- the question of whether the Framework Decision should also cover information which is transmitted to third States;

the question of whether the scope of the Framework Decision should be confined to the cross-border transmission of information and the processing of data thus transmitted or whether it should ? as envisaged in the Commission proposal ? also encompass data gathered and used in a purely domestic context.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The committee adopted the report by Martine ROURE (PES, FR) amending - under the consultation procedure - the proposed framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The key amendments were as follows:

- a new article stipulated that the further processing of personal data shall be allowed only ?for the specific purpose for which they were transmitted or made available?, ?if strictly necessary, 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?. The personal data concerned may be further transferred to another Member State only with the prior consent of the authority which made the information available in the first place;

- MEPs approved of the distinction made between the various types of data and the different treatment thereof, and they proposed adding a new clause stipulating that personal data relating to people who are not under suspicion should be processed ?only for the purpose for which they were collected, for a limited period of time, with adequate limitations on access to them and on their transmission?;

- a new clause laid down the principles of proportionality and necessity as criteria for establishing whether the processing of personal data is legitimate;

- additional specific safeguards should be introduced to protect particularly sensitive information such as biometric data and DNA profiles to ensure that such data are accurate and may be challenged by the data subject;

- the measures on time-limits for the storage of personal data should provide for automatic and regular deletion after a certain period of time;

- the committee amended the title of Section I of Chapter III to read ?Transmission of and making available personal data?, thereby ensuring that this section would apply to the processing of all data and not, as originally proposed, only to data exchanged between Member States. Moreover, some of the provisions laid down in Section II of Chapter III (on transmission to private parties and on transfer to competent authorities in third countries or to international bodies) were transferred to Section I;

- it was stipulated that the transmission of personal data to authorities other than the competent authorities of a Member State would be allowed only in ?particular individual and well-documented cases?;

- it should be possible to impose criminal sanctions on authorities not only for offences committed intentionally but also for offences committed through gross negligence. Moreover, private parties should also be subject to penalties under criminal law for any abuse of the data, particularly as regards confidentiality and security;

- lastly, MEPs wanted the data protection rules applicable to Europol, Eurojust and the Customs Information System (which were excluded from the proposal because they have their own data protection provisions) to be made fully consistent with the Framework Decision, and therefore called on the Commission to submit a proposal to this end within two years.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The European Parliament decided to postpone a report drafted by Martine ROURE (PSE, FR) endorsing the decision of the Legal Affairs Committee. Although MEPs believe the proposal will bring more uniformity and consistency to the EU´s data protection principles, they decided to wait until the Council meets again in July, hoping the Finnish presidency will be more willing to take into account Parliament's demands.

Even though the final vote was postponed, Parliament voted through all the 60 amendments tabled, approving them to make clear their support to the position of rapporteur and committee members. (For a summary of the main amendments, please refer to the document dated 15/05/2006.) In general, the amendments limit the use and access to personal data to the very necessary cases and when there is a real threat to public security.

The Commission proposal responds to an old claim from the Parliament, which, since the creation of the third pillar, has been calling for standards on data protection in the context of judicial and police cooperation. The issue is particularly relevant now that the European Court of Justice decided to annul existing agreements between the EU and US government on the transfer of personal data of air passengers flying into the United States. It is a priority for the Parliament to push for a quick adoption of this draft decision by the Council, which would affect future agreements with the USA.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The European Parliament adopted a resolution by Martine ROURE (PSE, FR) and endorsed the Commission proposal subject to several amendments designed to reinforce data privacy. (For a background to this resolution, please see the previous summary.) The Commission?s proposal would extend data protection rules as regards transfer of information in police and judicial cooperation.

Competence in this matter is currently solely a matter for Member States. More than 60 amendments were also adopted that limit the use and access to personal data in cases where there is a real threat to public security.

Parliament was concerned about the issue of access to personal data by non-EU countries. It adopted an amendment limiting such transfers to competent authorities outside the EU only if the transfer is provided by a law clearly obliging or authorising such a transfer. Member States must ensure that there is adequate data protection in the non-EU country based upon concrete criteria listed in the text. Only exceptionally could the adequacy condition be lifted in the event of an imminent serious danger.

Data collection and access for national governments or competent authorities must be limited to specific purposes, only if strictly necessary, and carried out with the principles of proportionality and necessity and for the purpose of preventing a threat to public security or to a person. This personal data made available to a given Member State might be further processed by another Member State only with the consent of the authority which made available the information in the first place. Sensitive data such us biometrics or DNA information will follow additional specific safeguards to ensure they are accurate and that they can be challenged by the subject of such data. Parliament wanted a different treatment for personal data depending on the status of the person concerned: information related to non-suspects will be treated only for the specific purpose they were collected, for a limited period of time and with adequate limitations on access to them and on their transmission.

Other amendments adopted give citizens the right to deny the accuracy of some personal information and mark it on the database. Competent authorities would be liable to criminal sanctions in case of intentional offence or gross negligence.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

Second Opinion of the European Data Protection Supervisor on the Proposal for a Council Frame-work Decision on the protection of personal data processed in the framework of policy and judicial co-operation in criminal matters.

Whilst welcoming Council efforts on the proposal for the protection of personal data processed in the framework of policy and judicial co-operation in criminal matters, the European Data Protection Supervisor (EDPS) nevertheless expresses some concern regarding the direction certain developments are taking. The texts currently being discussed within Council fail to incorporate amendments proposed by the European Parliament ? nor do the Council texts consider the first opinion of the EDPS. On the contrary, in quiet a few cases provisions in the Commission proposal that offer safeguards, have been deleted or substantially weakened. The EDPS warns that such weakening of safeguards could risk a level of protection that is lower than the level of protection afforded under Directive 95/46/EC or that of the more generally formulated Council of Europe Convention No 108, which is binding on the Member States. It is for these reasons that the EDPS is now issuing a second opinion.

Although the EDPS recognises the importance of adopting the Framework Decision as soon as possible, it nevertheless gives warning that a speedy solution should not be sought at the expense of lowering standards. The lack of time given to reaching a consensus should not result in the quality of the Framework Decision being compromised. Further, the protection afforded must be consistent and independent of where, by whom, or for which purpose personal data is processed. Common rules on data protection should apply to all data in the area of police and judicial co-operation, and not be limited to cross-border exchanges between Member States.

The EDPS opinion also argues that limiting the scope of the Framework Decision is unworkable and suggests that to limit the scope would result in additional complexity and increased costs. It could, in addition, harm the legal certainty of individuals.

Other concerns of the EDPS are:

- The specific provisions on data quality in the Commission proposal should not be deleted from the proposal. Nor should they be made optional.
- The Provisions on the further use of data and on special categories of data should be consistent with Directive 96/46/EC and in line with the Council of Europe Convention No 108.
- The specific provisions on data exchange, with parties other than law enforcement authorities within the EU, should not be deleted from the proposal, nor be limited in scope. As to the exchange of data with third countries, mechanisms should at the very least ensure common standards and co-ordinated decisions on adequacy are put in place. The text of the Framework Decision should provide for such mechanisms.
- Solutions making the right to information dependent upon a request by the data subject are not acceptable and are not compatible with Council of Europe Convention No 108.
- The position of the data protection authorities should be consistent with the position afforded to them under Directive 96/46/EC.
- The detailed rules on security, comparable to the rules included in the Europol-convention, should not be deleted from the proposal.

The Commission and the Council should adopt a proposal on processing specific categories of data, such as biometric data and DNA-profiles, whether related to the principle of availability or not.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The Council took note of the state-of-play concerning this file. The main fundamental outstanding question is whether this Framework Decision should also apply to domestic data processing, or only to cross-border data processing.

The position of the vast majority of delegations has so far been that any data gathered in the context of an internal investigation could, at a later stage, possibly be exchanged with foreign authorities and that therefore the scope of the Framework Decision should encompass all data. The opposing delegations thought the scope of the Framework Decision should be limited to the cross-border exchange of data.

This Framework Decision would determine common standards to ensure the protection of individuals with regard to the processing of personal data in the framework of police and judicial co-operation in criminal matters, provided for by Title VI of the Treaty on European Union, while safeguarding citizens' freedom and providing them with a high level of safety.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

On 4 October 2005, the Commission forwarded a proposal for a Council Framework Decision on the protection of personal data processed in

the framework of police and judicial cooperation in criminal matters ("DPFD") to the Secretary-General of the Council.

The Parliament delivered its opinion on 27 September 2006. The European Data Protection Supervisor has also delivered his opinion on the proposal, which he presented to the Multidisciplinary Group on Organised Crime (MDG)-Mixed Committee on 12 January 2006.

The Commission presented its proposal to the meeting of the MDG - Mixed Committee on 9 November 2005. The MDG discussed the proposal at length and completed the third reading at its meeting on 15 and 16 November 2006.

At a Council meeting, the Presidency set out a series of basic points for revising the proposal, with the aim of removing outstanding reservations and making a real improvement in third-pillar data protection.

The German Presidency is now submitting a revised draft Framework Decision draft which reflects those points.

The draft contains a new provision (Article 26) designed to replace the existing four data protection authorities within the third pillar by a single independent joint supervisory body, merging with it the advisory working party provided for in the earlier draft.

A separate Council Decision is necessary in order to establish that body. The Presidency intends as soon as possible to submit conclusions to the Council endorsing that aim and asking the Commission to bring forward a proposal for the relevant Council Decision.

The new draft Framework Decision provides that the joint supervisory authority:

- shall 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;

- 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.

Other than the creation of a joint supervisory authority, the new version of the draft Framework Decision:

- applies only to data gathered or processed by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

- applies the rules of the Framework Decision to national data-processing, in order that the conditions for transmitting data may already be met when the data are collected.

- allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Framework Decision.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

Third opinion of the European Data Protection Supervisor 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.

The European Data Protection Supervisor has already issued two opinions on the proposed Council Framework Decision regarding the protection of personal data processed in the framework of policy and judicial co-operation in criminal matters. (December 2005 and November 2006). In January 2007 the German Presidency set out a series of basic points to revise the proposal, with a view to removing any outstanding reservations and to improve data protection in the third pillar. The substantive changes contained in the revised proposal, as well as its importance, call for a new opinion of the EDPS.

Whilst welcoming the effort put into the proposal by the German Presidency, the EDPS nevertheless remain concerned that the text does not live up to expectations for the following reasons:

- The text weakens the level of citizens? protection, since the number of essential provisions for their protection have been removed.
- The revised proposal falls below the level of protection afforded by Convention 108. It is thus unsatisfactory and will be incompatible with Member States? international obligations.
- The text adds, rather than reduces, administrative complexities since it covers Europol, Eurojust and third-pillar Customs Information System? data processing.
- The legislative quality of the text is unsatisfactory. The choice of legal instruments aside, several provisions do not fulfil the requirements of common guidelines for the quality of drafting Community legislation. The text, argues the EDPS, is not clear, simple and precise, which makes it difficult for citizens to identify their rights and obligations unambiguously.
- The low level of protection afforded by the proposal cannot serve the creation of an area of freedom, security and justice in which law enforcement information can be exchanged between police and judicial authorities disregarding national borders. Indeed the proposal makes exchanges of information still subject to different national ?rules of origin? and ?double standards? that strongly affect efficiency in law enforcement co-operation while not improving the protection of personal data.

As a result of the above, the EDPS argues that the proposal needs to be revised substantially before it could form the basis for discussion on data protection in the third pillar. Any improvements should ensure that the Decision:

- provides added value to Convention 108 by laying down appropriate provisions on the protection of personal data required by Article 30(1) of the EU-Treaty.
- applies to domestic processing of personal data by law enforcement authorities;
- is consistent with first pillar data protection principles, whilst also taking account of the unique nature of law enforcement activities;
- is in line with the principles laid down by Convention 108 and Recommendation No R (87) 15. In particular with regard to: limiting the processing of personal data; the quality of data (including distinguishing between criminals, suspects, victims, witnesses etc.; assessment of the different degree of accuracy and reliability of personal data and mechanisms to ensure periodic verification and rectification.);

- ensures adequate protection in the exchange of personal data with third countries ? also with regard to international agreements; and
- addresses the other points mentioned in this, as well as, previous EDPS opinions.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The committee adopted the report by Martine ROURE (PES, FR) amending - under the consultation procedure, in the framework of a renewed consultation of Parliament on this dossier - the proposed Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters:

- a new recital stated that the Framework Decision was "merely the first step towards a more comprehensive and consistent framework for the protection of personal data used for security purposes", and that it should be based on the 15 principles attached to the proposal (which were the result of a trialogue between the rapporteur, the Council and the Commission);

- scope: the committee felt that the Framework Decision should apply to all national authorities without exception and therefore deleted Article 1(4) which would have excluded "authorities or other offices dealing specifically with matters of national security". It also added a new clause providing for the Commission to submit proposals after 3 years with a view to extending the scope of the Framework Decision to cover the processing of personal data within the framework of police and judicial cooperation at national level;

- subsequent processing of data: the committee amended the clause allowing for the processing of data "for any other purpose" as referred to in Article 12(1)(d), saying that personal data may be further processed only for a "specified" purpose, "provided that it is legitimate and not excessive" in relation to the purposes for which the data were collected;

- transfer of data to third countries: the committee specified that personal data can be transferred to third countries or international organisations only if this is necessary for the "prevention, investigation, detection or prosecution of terrorist offences and other serious criminal offences", if this complies with the national law of the Member State from which the data were obtained and if the country or organisation concerned ensures an adequate level of protection for the intended data processing. However, it will be possible to transfer data in exceptional circumstances, "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", even if the third country does not guarantee an adequate level of protection;

- transfer of data to authorities other than competent authorities: this should be allowed only "in particular individual and well-founded cases" and if it is necessary for preventing, investigating, detecting or prosecuting criminal offences or for preventing threats to public security or to a person;

- transfer of data to private persons and access to data relating to private persons: the committee adopted provisions aimed at strictly regulating the communication of personal data to private persons, which should be clearly authorised. When collecting and processing such data as part of a public service remit, private persons should be subject, at least, to the same conditions on data security as apply to the competent public authorities. Members of the public have the right to be informed if their personal data are used;

- the content and accuracy of personal data: personal data shall be evaluated taking into account "their degree of accuracy or reliability [...]" Data which are inaccurate or incomplete should be erased or rectified. Member States should ensure that data "is verified regularly in order to ensure that the data accessed are accurate and up to date";

- national authorities: the joint supervisory authority established by the Framework Decision should bring together the national supervisory authorities and the European Data Protection Supervisor;

- assessment and revision: a new article provided for the Commission to submit an assessment of the application of the Framework Decision after 3 years to Parliament and Council, together with propsals for amendments where necessary.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The European Parliament adopted a resolution drafted by Martine ROURE (PES, FR) amending-in the framework of a renewed consultation of Parliament on this dossier - the proposal on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The principal amendments were as follows:

- new recitals state that the 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. With a view to ensuring that the international obligations of the Member States are fulfilled, the 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 EU, 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.

- a further new recital states that the 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 annexed to it, which were the result of a trialogue between the rapporteur, the Council and the Commission;

- scope: Parliament felt that the Framework Decision should apply to all national authorities without exception and therefore deleted Article 1(4) which would have excluded "authorities or other offices dealing specifically with matters of national security". It also added a new clause providing for the Commission to submit proposals after 3 years with a view to extending the scope of the Framework Decision to cover the processing of personal data within the framework of police and judicial cooperation at national level;

- the definition of "the data subject's consent" was deleted;

- the content and accuracy of personal data: 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. 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 under specified circumstances. 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. Member States shall ensure that the quality of personal data made available to the competent authorities of other Member States is verified regularly. Personal data that are no longer accurate or up to date must be neither transmitted nor made available.

- Parliament inserted a number of exceptions to the general prohibition on 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;

- subsequent processing of data: Parliament amended the clause allowing for the processing of data "for any other purpose" as referred to in Article 12(1)(d), saying that personal data may be further processed only for a "specified" purpose, "provided that it is legitimate and not excessive" in relation to the purposes for which the data were collected;

- transfer of data to third countries: Parliament specified that personal data can be transferred to third countries or international organisations only if this is necessary for the prevention, investigation, detection or prosecution of terrorist offences and other serious criminal offences", if this complies with the national law of the Member State from which the data were obtained and if the country or organisation concerned ensures an adequate level of protection for the intended data processing. However, it will be possible to transfer data in exceptional circumstances, 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, even if the third country does not guarantee an adequate level of protection;

- transfer of data to authorities other than competent authorities: this should be allowed only in particular individual and well-founded cases and if certain prescribed requirements are met;

- transfer of data to private persons and access to data relating to private persons: Parliament adopted provisions aimed at strictly regulating the communication of personal data to private persons, which should be clearly authorised. When collecting and processing such data as part of a public service remit, private persons should be subject, at least, to the same conditions on data security as apply to the competent public authorities. Members of the public have the right to be informed if their personal data are used;

- the joint supervisory authority shall gather the national supervisory authorities provided for in the Framework Decision and the European Data Protection Supervisor;

- assessment and revision: not more than three years after the date of entry into force of the Framework Decision, the Commission shall submit to the European Parliament and the Council an assessment of its application, accompanied by proposals for any amendments which are necessary in order to extend its scope;

- lastly, an annex contains the principles on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, referred to above.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The Council adopted the following conclusions on the protection of personal data relating to police and judicial cooperation in criminal matters.

In particular, it:

- recognizes the importance of the existence of a comprehensive and coherent set of rules at the level of the European Union concerning the high level of protection of personal data processed in the framework of police and judicial cooperation in criminal matters, as a part of the Union?s ever increasing set of regulatory instruments on such cooperation. These rules will build upon the minimum data protection principles set by the Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data and its Additional Protocol of 8 November 2001, and take account of Recommendation (87)15 regulating the use of personal data in the police sector, both adopted in the framework of the Council of Europe;

- notes that the European Parliament has rapidly forwarded its opinion on the revised draft of the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters and will examine all solutions suggested by the European Parliament, in the spirit of cooperation that is reflected in the opinion;

- will examine all solutions suggested by the European Parliament, in the spirit of cooperation that is reflected in its opinion of 24 May 2007. It will take note of the general principles in the annex to the opinion. The Council will take these principles, where appropriate, into consideration, when drafting the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters;

- continues to give priority to the examination of the proposal for a Council Framework Decision and intends to reach a political agreement on the proposal as soon as possible and at the latest by the end of 2007.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The Mixed Committee agreed on the scope of this draft Framework Decision and on the data protection regime for transfer of data to third countries.

The Council preparatory bodies will continue the examination of the rest of the text with a view to reaching an agreement as soon as possible.

After more than a year and a half of intense negotiations on this proposal, the Presidency proposed a narrow scope for the Framework Decision, which means that the text will apply to the cross-border exchange of personal data only. This understanding will also imply an evaluation by the Commission of the data protection system, including the limitation of the scope, three years after the Framework Decision will apply to Member States.

As regards the principles relating to the transmission of personal data to third States, data transmitted to another Member State may be transferred to third States or international bodies only if a number of conditions, including prior consent, are met.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

Pending the lifting of some parliamentary scrutiny reservations, the Mixed Committee agreed on a general approach on a proposal for a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

The text agreed envisages that the exchange of personal data will be supported by clear binding rules enhancing mutual trust between the competent authorities. Relevant information will be protected in a way excluding any obstruction of this cooperation between the Member States while fully respecting the fundamental rights of individuals, in particular the right to privacy and to protection of personal data. Common standards on the confidentiality and security of the processing, on liability and sanctions for unlawful use will contribute to achieving both aims.

In particular, the text defines the right of access to data, the right to rectification; erasure or blocking, the right to compensation and the right to seek judicial remedies.

This Framework Decision does not preclude Member States from providing safeguards for the protection of personal data higher than those established in this Framework Decision.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The Council reached a political agreement on the proposed Framework Decision which is significantly different to both the original Commission proposal and the Council text on which the European Parliament was first reconsulted. The Council has thus decided to proceed with a second reconsultation of the European Parliament based on the text which gained the political agreement of the Member States.

The purpose of this legislation is to ensure a high level of protection for the basic rights and freedoms, and in particular the privacy of individuals, while guaranteeing a high level of public safety when exchanging personal data.

The text agreed envisages that the exchange of personal data will be supported by clear binding rules, enhancing mutual trust between the competent authorities. Relevant information will be protected in a way excluding any obstruction of this cooperation between the Member States while fully respecting the fundamental rights of individuals, in particular the right to privacy and to protection of personal data. Common standards on the confidentiality and security of the processing, on liability and sanctions for unlawful use, will contribute to achieving both aims.

In particular, the text defines the right of access to data, the right to rectification; erasure or blocking, the right to compensation and the right to seek judicial remedies.

This Framework Decision does not preclude Member States from providing safeguards for the protection of personal data higher than those established in this Framework Decision.

The file was discussed at the Council meeting of 18 September 2007 and an agreement was reached on the regime for onward transfer on personal data obtained from another Member State to third States. The Council also confirmed the understanding that the text applies to the cross-border exchange of personal data only. The Commission will carry out an assessment of the data protection system, particularly the limit of its scope, three years after the date on which the Member States apply the Framework Decision.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The Committee on Civil Liberties, Justice and Home Affairs adopted a report drafted by Martine ROURE (PES, FR) on the renewed consultation regarding 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.

To recall, the European Parliament has been consulted twice on this subject: once in September 2006 and a second time June 2007. After deadlock in the Council on this framework decision, a third and final version of the text is now the subject to a renewed consultation based on the political agreement reached by the Council on 11 December 2007. The text is significantly different to both the original Commission proposal and the Council text on which the European Parliament was first reconsulted.

It made several amendments to the Council's text:

Convention 108: Member States must seek to ensure a high level of protection within the Union in accordance with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention108").

Definitions: the committee tightened up the definition of "to make anonymous".

Scope: the committee felt that it was of crucial importance that the Framework Decision also applies to national data processing as to avoid different levels of data protection throughout the European Union. It therefore deleted the Commission's exclusion of national data. It also deleted the article in the Commission's text which stated that the Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security. 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 is prohibited. However, the Committee has specified certain exceptions. It added that these specific categories of data may not be processed automatically unless domestic law provides appropriate safeguards. The same proviso shall also apply to personal data relating to criminal convictions.

Insuring the principles of proportionality and purpose limitation: the committee notes that Article 3 sets the conditions for purpose limitation and proportionality. The collection of personal data must be fair and lawful as set out by article 9 of the Convention 108. Further processing will only be possible on a case by case basis in order to take into account the specific nature of police and judicial cooperation but only if it is compatible with the purposes for which the data was collected.

Article 12 (d) however allows for the data to be used for "any other purpose" which the committee considered too wide. Accordingly, personal data may only be further processed, inter alia, for any specified purpose provided that it is laid down by law and is necessary in a democratic society for the protection of one of the interests set out in Article 9 of Convention 108.

Transfer of data: more restrictive measures: following the Council?s approach, MEPs accept that transfer of data without prior consent shall be permissible only if transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and the prior consent cannot be obtained in good time. In such a case, the personal data may be processed by the recipient only if absolutely necessary for the specific purpose for which the data were supplied. The authority responsible for giving consent shall be informed without delay. Such data transfers shall be notified to the competent supervisory authority.

Transmission to private parties and access to data received by private parties in Member States: a new clause states that Member States shall provide that their respective competent authorities may have access to and process personal data controlled by private persons only on a case-by-case basis, in specific circumstances, for specified purposes and subject to judicial scrutiny in the Member States.

The national legislation of the Member States shall provide that, where private persons receive 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.

Transmission to third countries: Member States shall provide that personal data transmitted or made available on a case-by-case basis by the competent authority of another Member State may be transferred to third States or international bodies only under certain circumstances and, inter alia, if the third State or international body concerned ensures an adequate level of protection for the intended data processing equivalent to the one afforded by Article 2 of the Additional Protocol to the Convention 108 , and the corresponding case-law under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Supervisory authorities: each Member State shall ensure that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences or the enforcement of criminal penalties.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data: the committee inserted a new article providing that a Working Party on the Protection of Individuals with regard to the Processing of Personal Data for the purpose of the Prevention, Investigation, Detection and Prosecution of Criminal Offences, be established with advisory status and act independently. The Working Party?s main task shall be to give an opinion on national measures, where necessary to ensure that the standard of data protection achieved in national data processing as well as on the level of protection between the Member States and third countries and international bodies.

Commission's report: this must take into account the observations forwarded by the parliaments and governments of the Member States, the European Parliament, the Article 29 working party established by Directive 95/46/EC, the European Data Protection Supervisor and the Working Party established in Article 25a of this Framework Decision.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The European Parliament adopted, by 600 votes in favour to 21 against with 9 abstentions, a legislative resolution on the renewed consultation regarding 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. The report had been tabled for consideration by Martine ROURE (PES, FR) on behalf of the Committee on Civil Liberties, Justice and Home Affairs.

To recall, the European Parliament has been consulted twice on this subject: once in September 2006 and a second time June 2007. After deadlock in the Council on this framework decision, a third and final version of the text is now the subject to a renewed consultation based on the political agreement reached by the Council on 11 December 2007. The text is significantly different to both the original Commission proposal and the Council text on which the European Parliament was first re-consulted.

Parliament made several amendments to the Council's text:

Convention 108: Member States must seek to ensure a high level of protection within the Union in accordance with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention108").

Definitions: the committee tightened up the definition of "to make anonymous".

Scope: Members felt that it was of crucial importance that the Framework Decision also applies to national data processing as to avoid different levels of data protection throughout the European Union. They deleted the Commission's exclusion of national data. They also deleted the article in the Commission's text which stated that the Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security. 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 is prohibited. However, Parliament has specified certain exceptions. It added that these specific categories of data may not be processed

automatically unless domestic law provides appropriate safeguards. The same proviso shall also apply to personal data relating to criminal convictions.

Ensuring the principles of proportionality and purpose limitation: the collection of personal data must be fair and lawful as set out by article 9 of the Convention 108. Further processing will only be possible on a case by case basis in order to take into account the specific nature of police and judicial cooperation but only if it is compatible with the purposes for which the data was collected.

Article 12 (d) however allows for the data to be used for "any other purpose" which Parliament considered too wide. Accordingly, personal data may only be further processed, inter alia, for any specified purpose provided that it is laid down by law and is necessary in a democratic society for the protection of one of the interests set out in Article 9 of Convention 108.

Transfer of data: more restrictive measures: following the Council?s approach, MEPs accept that transfer of data without prior consent shall be permissible only if transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and the prior consent cannot be obtained in good time. In such a case, the personal data may be processed by the recipient only if absolutely necessary for the specific purpose for which the data were supplied. The authority responsible for giving consent shall be informed without delay. Such data transfers shall be notified to the competent supervisory authority.

Transmission to private parties and access to data received by private parties in Member States: a new clause states that Member States shall provide that their respective competent authorities may have access to and process personal data controlled by private persons only on a case-by-case basis, in specific circumstances, for specified purposes and subject to judicial scrutiny in the Member States.

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

Transmission to third countries: Member States shall provide that personal data transmitted or made available on a case-by-case basis by the competent authority of another Member State may be transferred to third States or international bodies only under certain circumstances and, inter alia, if the third State or international body concerned ensures an adequate level of protection for the intended data processing equivalent to the one afforded by Article 2 of the Additional Protocol to the Convention 108 , and the corresponding case-law under Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms.

Supervisory authorities: each Member State shall ensure that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences or the enforcement of criminal penalties.

Working Party on the Protection of Individuals with regard to the Processing of Personal Data: Parliament inserted a new article providing that a Working Party on the Protection of Individuals with regard to the Processing of Personal Data for the purpose of the Prevention, Investigation, Detection and Prosecution of Criminal Offences, be established with advisory status and act independently. The Working Party?s main task shall be to give an opinion on national measures, where necessary to ensure that the standard of data protection achieved in national data processing as well as on the level of protection between the Member States and third countries and international bodies.

Commission's report: this must take into account the observations forwarded by the parliaments and governments of the Member States, the European Parliament, the Article 29 working party established by Directive 95/46/EC, the European Data Protection Supervisor and the Working Party established in Article 25a of this Framework Decision.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

PURPOSE: to ensure a high level of protection of fundamental rights, and in particular the right to privacy, with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters.

LEGISLATIVE ACT: Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

CONTENT: the Council adopted a Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. The purpose of this act is to ensure a high level of protection for the basic rights and freedoms, and in particular the privacy, of individuals, while guaranteeing a high level of public safety when exchanging personal data.

The Framework Decision sets out principles of lawfulness, proportionality and purpose. It provides that personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected. Further processing for another purpose is only permitted under specified circumstances.

The Framework Decision defines, among other things:

- the right of access to data;
- the right to rectification, erasure or blocking;
- the right to compensation and the right to seek judicial remedies. It does not preclude Member States from providing higher-level safeguards for protecting personal data than those established in the framework decision.

Transfer to competent authorities in third States or to international bodies: the legislation provides that personal data transmitted or made available by the competent authority of another Member State may be transferred to third States or international bodies, only under certain circumstances, inter alia, that the Member State from which the data were obtained has given its consent to transfer in compliance with its national law; and the third State or international body concerned ensures an adequate level of protection for the intended data processing.

National supervisory authorities: each Member State must provide that one or more public authorities are responsible for advising and monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Framework Decision. These authorities shall act with complete independence in exercising the functions entrusted to them.

Evaluation: Member States shall report to the Commission by 27/11/ 2013 on the national measures they have taken to ensure full compliance with the Framework Decision, and particularly with regard to those provisions that already have to be complied with when data is collected.

ENTRY INTO FORCE: 20/01/2009.

TRANSPOSITION: 27/11/2010. The Council shall, before 27/11/2011, assess the extent to which Member States have complied with the provisions of this Framework Decision.

Fight against terrorism: processing and protection of personal data in the framework of police and judicial cooperation in criminal matters. Framework Decision

The Commission presents a report taking stock of the state of implementation of Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

The main points of the report are as follows:

Scope of national implementation measures: the Framework Decision applies only to the processing of personal data transmitted or made available between Member States (Article 1(2)). Processing personal data by police and justice in criminal matters at national level does not fall within the scope of the Framework Decision.

Three Member States considered the limited scope of the Framework Decision as problematic. Italy and the Netherlands reported difficulties in distinguishing in practice between cross-border processing of data under Framework Decision 2008/977 and processing at national level, and the related complexity for law enforcement authorities in Member States to cope with different processing rules for the same personal data. Poland pointed to the deficiencies of the Framework Decision in general and, in particular, stressed its support for the Commission's aim to establish a comprehensive framework and the extension of general data protection rules to the area of police and judicial cooperation in criminal matters.

Information to data subjects (Article 16): under the Framework Decision, Member States must ensure that their competent authorities inform data subjects that their data are being processed or transmitted to another Member

State. Almost all Member States indicated that they provide data subjects with some information on the processing of their personal data. France indicated that it does not do so. Denmark does not grant this right either, but reported that the controller must keep a register and inform the public.

The right of information is subject to limitations in the vast majority of Member States.

The Netherlands stated that a general obligation to inform the data subject was not entirely consistent with the nature of the work of the police and judiciary, but that certain arrangements are in place to make sufficient provision for informing the data subject as required on data processing by the police and judicial authorities.

The Netherlands also stated that this provision need not be implemented because Article 16(1) merely refers to national laws of Member States.

The Framework Decision establishes data subjects right to information but does not contain any details on the methods or on possible exemptions. Even if, according to the Member States, the right to information is generally granted, implementation varies considerably.

Right of access of data subjects (Article 17): the Framework Decision contains general rules providing data subjects with the right to access their data. It does not specify in detail what kind of information needs to be given to the data subject. It also leaves it to Member States to decide whether data subjects may exercise their right of access directly or whether they must use the indirect route.

All Member States grant some form of right of access to data subjects. Equally, all Member States provide for exemptions from the right of access. The most frequently mentioned reasons for not granting the right of access include the prevention, investigation and prosecution of criminal offences and national security, defence and public security.

Other issues raised by Member States: 6 Member States made comments on issues of concern to them:

- Poland considered that the Framework Decision contained numerous deficiencies, which should be remedied, and expressed support for reform in order to establish a comprehensive and coherent data protection system at EU level;
- Italy and the Netherlands raised a difficulty in distinguishing in practice between cross-border processing of data under Framework Decision 2008/977 and processing at national level, and the related difficulty for law enforcement authorities in Member States to cope with different processing rules for the same personal data;
- Italy, the Czech Republic and the Netherlands expressed criticism towards the rules on international transfers included in the Framework Decision. In particular, Italy said that it was necessary to provide for an adequate and more uniform level of data protection for data transfers to third countries. The Netherlands considered problematic the lack of criteria in the Framework Decision to determine the adequate level of protection of a third country, leading to variable implementation by Member States. The Czech Republic considered the rules on international transfers in the Framework Decision as 'unrealistic';
- France referred to a specific problem at national level in relation to the storage periods of personal data transmitted to and from a third country having different requirements in that respect;
- Slovakia said it was necessary to differentiate more between data processing by the police and by the judiciary (court proceedings);
- the Czech Republic and the Netherlands indicated that it was confusing for law enforcement to have to comply with multiple data protection rules at international (such as the Council of Europe), EU and national level.

The report considers that the practical difficulties encountered by a number of Member States in distinguishing between rules for domestic and cross-border data processing, could be solved through a single set of rules covering data processing both at national level and in a cross-border context. The scope and possible exemptions at EU level regarding the data subjects right to information would merit further

clarification. Minimum harmonised criteria regarding data subjects right of access could strengthen the rights of data subjects while also providing exemptions to allow the police and justice to properly perform their tasks.

Under Article 16 of the Treaty on the Functioning of the European Union, which enshrines the right to the protection of personal data, there is now the possibility of establishing a comprehensive data protection framework ensuring both a high level of protection of individuals data in the area of police and judicial cooperation in criminal matters and a smoother exchange of personal data between Member States police and judicial authorities, fully respecting the principle of subsidiarity.