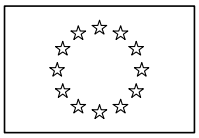

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 04.08.2005
COM (2005)

Proposal for a

COUNCIL FRAMEWORK DECISION

on the protection of personal data processed in the course of activities of police and judicial co-operation in criminal matters provided for by Title VI of the Treaty on European Union

EN

EXPLANATORY MEMORANDUM

1) CONTEXT OF THE PROPOSAL

- **Grounds for and objectives of the proposal**

On 4 November 2004, the European Council adopted The Hague Programme on strengthening freedom, security and justice in the European Union.[1] In The Hague Programme the Commission is invited to submit proposals by the end of 2005 at the latest for the implementation of the principle of availability in order to improve the cross-border exchange of law-enforcement information between the Member States. The Hague Programme stresses that key conditions in the area of data protection should be strictly observed in these proposals.

In the meeting on 2 and 3 June 2005, the Council and the Commission adopted the Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union.[2] The Action Plan was based on the Communication from the Commission to the Council and the European Parliament - The Hague Programme: Ten priorities for the next five years. The Partnership for European renewal in the field of Freedom, Security and Justice.[3] The Action Plan sets out the list of legislative and non-legislative measures which the Council and the Commission consider necessary to put into practice the guidelines set in the Hague Programme. This list includes *proposals to be submitted in 2005 on (1) the establishment of a principle of availability of law enforcement relevant information and (2) on adequate safeguards and effective legal remedies for the transfer of personal data for the purpose of police and judicial cooperation in criminal matters.*

On 13 July 2005, the Council (Justice and Home Affairs) in its Declaration on the EU response to the London bombings[4] called on the Commission to present proposals on data protection principles in the field of law enforcement and, in accordance with the Hague programme, on the principle of availability by October 2005.

This Framework Decision shall, in addition to the Framework Decision on the exchange of information under the principle of availability, determine rules for protection of personal data processed in the course of activities of police and judicial co-operation in criminal matters provided for by Title VI of the Treaty on European Union . It aims at improving police and judicial cooperation in criminal matters, in particular regarding the preventing and combating terrorism, between the Member States of the European Union (third pillar) and at the strict observance of key conditions in the area of data protection. It shall ensure that, in particular in view of the implementation of the principle of availability, throughout the European Union fundamental rights , with special attention to the right to privacy and to the protection of personal data, will be respected and that the exchange of relevant information between the Member States will not be hampered by different levels of data protection in the Member States.

1 OJ C 53, 3.3.2005, p. 1

2 Council Working Document 9778/2/05 REV 2 JAI 207

3 COM(2005) 184 final, Brussels, 10.5.2005

4 Council Working Document 11158/1/05 REV 1 JAI 255

- **General context**

Common standards for the processing and protection of personal data in the third pillar were already discussed in 1998. On 3 December 1998, the Council (Justice and Home Affairs) adopted the Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice.[5] The plan stipulated that - with regard to horizontal problems in the context of police and judicial cooperation in criminal matters - the possibilities for harmonised rules on data protection should be examined within two years from the entry into force of the Treaty. In 2001, first efforts ended without success when no agreement could be achieved on a Draft Resolution on the personal data protection rules in instruments under the third pillar of the European Union.[6]

The debate, however, continued.In June 2003 the Greek Council Presidency presented a set of 12 principles on personal data protection in the third pillar in order to create a common European policy I this regard inspired by the general data protection Directive 95/46/EC and the Charter of Fundamental Rights of the European Union.

[PM: Italian initiative]

Finally, in 2005, the Data Protection Authorities of all Member States of the European Union and the European Data Protection Supervisor strongly supported a new legal instrument for data protection in the third pillar (Declaration and Position paper on law enforcement and information exchange in the EU, adopted by the Spring Conference of European Data Protection Authorities, Krakow, 25-26 April 2005). The European Parliament recommended harmonising existing rules on the protection of personal data in the instruments of the third pillar, bringing them together in a single instrument that guarantees the same level of data protection as provided for under the first pillar (No. 1 h of European Parliament recommendation to the European Council and the Council on the exchange of information and cooperation concerning terrorist offences (2005/2046(INI)), adopted on 7 June 2005).

According to The Hague Programme, the introduction of the principle of availability is dependent on key conditions in the area of data protection. Obviously, the European Council acknowledged that data protection provisions presently existing at European level would not be sufficient in view of the implementation of the principle of availability, which might include modalities such as reciprocal access to or interoperability of national databases or direct (on-line) access.

Concerns about a sufficient level of data protection were also reflected in a cooperation agreement signed by seven Member States on 27 May 2005 (Germany, Austria, Belgium, the Netherlands, Luxembourg, France, and Spain) and which they recommend as a model for the exchange of information between the Member States of the Union in general. The agreement provides, subject to specific conditions, for direct automated access for the law enforcement authorities of one Contracting Party to personal data hold by another Contracting Party. But this form of cooperation shall not apply until the data protection provisions of the agreement have been transposed into the national law of the Parties.

- **Existing provisions in the area of the proposal**

5 OJ C 19, 23.1.1999, p. 1

6 Council Working Document 6316/2/01 REV 2 JAI 13

Article 8 of the Charter of Fundamental Rights of the European Union explicitly recognises that everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

The Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[7] contains fundamental rules on the lawfulness of the processing of personal data as well as 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, a specific supervisory authority and 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). Insofar 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. Provisions on the protection of personal data are included in instruments adopted under Title VI of the TEU that organise the exchange of information between customs, police and judicial authorities of Member States, in particular in instruments that establish common information systems at European level, such as: the Convention implementing the Schengen Agreement of 1990 including specific data protection provisions applicable to the Schengen Information System;[8] the Europol Convention of 1995[9] and, inter alia, the Rules governing the transmission of personal data by Europol to third States and third bodies;[10] the Decision setting up Eurojust of 2002[11] and the Rules of procedure on the processing and protection of personal data at Eurojust;[12] the Convention on the use of information technology for customs purposes of 1995, including personal data protection provisions applicable to the Customs Information System;[13] furthermore the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000, in particular Article 23.[14] With regard to Schengen Information System particular attention has to be paid to the establishment, operation and use of the second generation Schengen information system (SIS II), for which the Commission already submitted proposals for a Council Decision[15] and for two Regulations.[16]

Furthermore, attention has to be paid to the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981, to its Additional Protocol of 2001 regarding supervisory authorities and transborder data flows and to the Recommendation No. R (87) 15 of 1987 regulating the use of personal data in the police sector. All Member States are parties to the Convention but not all MS are parties to the Additional Protocol.

7 OJ L 281, 23.11.1995, p. 31

8 OJ L 239 , 22.9.2000, p. 19

9 OJ C 316, 27.11.1995, p. 2

10 OJ C 88, 30.3.1999, p. 1

11 OJ L 63, 6.3.2002, p. 1

12 OJ C 68, 19.3.2005

13 OJ C 316, 27.11.1995, p. 34

14 OJ C 197, 12.7.2000, p. 1, 15

15 COM (2005) 230 final

16 COM (2005) 236 final, COM (2005) 237 final

- **Consistency with the other policies and objectives of the Union**

The specificities of data processing and data protection in the course of activities provided for by Title VI of the Treaty on European Union have to be recognised. On the one hand, they should not hamper consistency with the general policy of the Union in the area of data protection on the basis of the EU Charter for Fundamental Rights and of Directive 95/46/EC. The fundamental principles of data protection apply to data processing in the first and in the third pillar. Moreover, consistency must be ensured with other instruments providing for specific obligations related to information that is likely to be relevant for the purpose of preventing and combating crime. Particular attention has to be paid to the development regarding the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.

2) CONSULTATION OF INTERESTED PARTIES AND IMPACT ASSESSMENT

- **Consultation of interested parties**

Consultation methods, main sectors targeted and general profile of respondents
On 22 November 2004 and on 21 June 2005, the Commission invited and consulted experts representing the Governments of Member States and of Iceland, Norway and Switzerland. On 11 January 2005, the Commission convened a consultative meeting with the Data Protection Authorities of these States. The European Data Protection Supervisor, Europol, Eurojust, and the Secretariat of the Joint Supervisory Bodies were involved. Some consulted parties sent written comments to the Commission. The main purpose of the consultations was to find out the need for a legal instrument on the processing and protection of personal data in the third pillar and, if so, what the main content of such an instrument should be. The Commission asked the consulted parties, inter alia on the basis of a questionnaire and a discussion paper, about their position concerning the general approach of a new legal instrument and its relation to existing instruments, the legal basis, the possible scope, the principles relating to data quality, the criteria for making data processing by police or judicial authorities legitimate, personal data of non-suspects, the requirements for the transmission of personal data to competent authorities in other Member States and in third countries, the rights of the data subject, supervisory authorities and a possible advisory body for data protection in the third pillar.

The Working Party set up according to Article 29 of Directive 95/46/EC was regularly informed about the ongoing development. On 12 April and 21 June 2005, the Commission attended meetings of the Police Working Party of the Conference of the European Data Protection Authorities. On 31 January 2005, the Commission participated in a "Public Seminar: Data protection and citizens' security: what principles for the European Union?" held by the Committee on Civil Liberties, Justice and Home Affairs. The Commission took into account the results of the Spring Conference of the European Data Protection Authorities, Krakow, 25-26 April 2005, and the position of the European Parliament as set out, inter alia, in the European Parliament recommendation to the European Council and the Council on the exchange of information and cooperation concerning terrorist offences (2005/2046(INI)), adopted on 7 June 2005.

All consulted interested parties without exception were in favour of a new legal instrument that harmonises data protection standards for information exchange for police and judicial cooperation in criminal matters..

Summary of responses and how they have been taken into account

Both the European Parliament and the Data Protection Authorities in the European Union strongly support a legal instrument providing for common standards for the processing and the protection of personal data in the third pillar. Representatives of the Governments of the Member States and of Iceland, Norway and Switzerland, furthermore of Europol and Eurojust did not express a common position in that regard. But the Commission could conclude that there was no principal opposition to the idea of such an instrument. There seemed to be agreement that the implementation of the principle of availability has to be accompanied by appropriate counterbalancing rules in the area of data protection. In that context, some Member States stated that the way information is exchanged in the future should be defined first and that rules for the processing and protection of personal data should be laid down subsequently. Some preferred a set of specific provisions to be included in the act on the principle of availability.

Having weighed up the different positions 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 highly 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 due 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 be accompanied by strict obligations to constantly ensure and verify the quality of data to which direct automated access is granted.

With special attention to gthe impact of the implementation of the principle of availability, provisions just addressing individual aspects of data processing and protection are not sufficient. A legal instrument providing for common standards for the processing and protection of personal data in the third pillar can, in principle, contribute to fostering police and judicial cooperation in criminal matters with regard to its efficiency as well as its legitimacy and compliance with fundamental rights, in particular the right to protection of personal data.

In particular in with a view to the implementation of the principle of availability such instrument is particularly necessary and must be developed hand in hand with the implementation of the principle of availability. The Framework Decision should follow the spirit and structure of Directive 95/46/EC as far as possible while taking into account the specific needs of police and judicial cooperation in criminal matters and in the light of the principle of proportionality. The Recommendation Nr R(87)15 regulating the use of personal data in the police sector of the Council of Europe of 1987 has been taken into account in order to transpose its main principles into legally binding provisions at EU level. Clear rules should be established for the processing 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 the data concerned. Such 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.

- **Impact assessment**

The following options were considered: applicability of Directive 95/46/EC; no or later proposal for provisions on the processing and protection of personal data in the third pillar; limited set of specific provisions in a legal act concerning the exchange of information under the principle of availability, Framework Decision on the protection of personal data in the third pillar. With regard to the latter it has been examined if such an instrument should also apply to the exchange of information through information systems and bodies established at EU level.

The fundamental and comprehensive provisions of Directive 95/46/EC are not applicable in the third pillar as set out in its Article 3(2). Even the deletion of this article could not automatically result in the applicability of the Directive on police and judicial cooperation in criminal matters. Firstly, the specificities of this cooperation are not fully taken into account in the Directive and would require some more preciseness. Secondly, the requirements for legislation according to Title VI of the Treaty of the European Union, which aim at fostering police and judicial cooperation in criminal matters, have to be respected The option of no or a later proposal for provisions on the processing and protection of personal data in the third pillar has to be excluded. This option is likely to imply that new forms of the exchange of information are introduced with the implementation of the principle of availability without ensuring strict observance of key conditions in the area of data protection. A limited set of specific provisions in a legal act concerning the exchange of information under the principle of availability is not sufficient given the probable impact of the latter. A Framework Decision on the protection of personal data processed in the course of activities of police and judicial co-operation in criminal matters provided for by Title VI of the Treaty on European Union is the only fully satisfying option.

The Commission carried out an impact assessment listed in the Work Programme, whose report is accessible on ….

3) LEGAL ELEMENTS OF THE PROPOSAL

- **Summary of the proposed action**

The proposed Framework Decision includes general rules on the lawfulness of processing of personal data, provisions concerning specific forms of processing (collection, storage, transmitting and making available 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 and 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 must 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.

- **Legal basis**

This Framework Decision shall be based on Articles 30, 31 and 34 (2) (b) of the Treaty on European Union. In particular in the light of the implementation of the principle of availability, appropriate provisions regarding the processing and protection of personal data, including common standards for the transmission of personal data to third countries and international bodies, are essential to improve police and judicial cooperation criminal matters, in particular for the fight against terrorism and serious crimes. Moreover, Member States will only fully trust each other if there are clear and common rules for the possible further transmission of exchanged data to other parties, in particular in third countries. The proposed provisions will ensure that the exchange of information between the competent authorities is not prejudiced by different levels of data protection in the Member States.

- **Subsidiarity and proportionality principle**

This Framework Decision addresses situations that are particularly relevant for police and judicial cooperation in criminal matters between the Member States, in particular for the exchange of information in order to ensure and promote efficient and lawful measures to prevent and combat crime, in particular serious crime and terrorism, in *all* Member States. National, bilateral or multilateral solutions might be helpful for individual Member States but would disregard to necessity of ensuring internal security for the whole Union. Therefore, this Framework Decision respects the principle of subsidiarity provided for by Article 2 of the Treaty on European Union and Article 5 of the Treaty establishing the European Community insofar as it aims to approximate the laws and regulations of the Member States, which cannot be done adequately by the Member States acting unilaterally and requires concerted action in the European Union. In accordance with the principle of proportionality, as set out in the latter Article, this Decision does not go beyond what is necessary in order to achieve that objective.

- **Choice of instruments**

Proposed instrument: framework decision. This legal instrument aims at the approximation of the laws and regulations of the Member States regarding the processing and protection of personal data processed for the purpose of preventing and combating crime.

4) BUDGETARY IMPLICATION

The implementation of the proposed Framework Decision would entail only low additional operational expenditure for meetings of and the secretarial services for the advisory body to be established according to Article 34 to be charged to the budget of the European Communities.
[Financial statement]

Proposal for a

COUNCIL FRAMEWORK DECISION

on the protection of personal data processed in the course of activities of police and judicial co-operation in criminal matters provided for by Title VI of the Treaty on European Union

THE COUNCIL OF THE EUROPEAN UNION,

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 proposal from the Commission,[(1)]

Having regard to the opinion of the European Parliament,[(2)]

Whereas,

(1) The European Union has set itself the objective to maintain and develop the Union as an area of freedom, security and justice; a high level of safety shall be provided by common action among the Member States in the fields of police and judicial cooperation in criminal matters. The European Union is founded on the principles of liberty, democracy, respect for human rights and fundamental freedoms, and the rule of law.

(2) According to Article 30 (1) (b) of the Treaty on European Union, common action in the field of police cooperation shall include the collection, storage, processing, analysis and exchange of relevant information subject to appropriate provisions on the protection of personal data. According to Article 31 (1) (a) of the Treaty on European Union, common action on judicial cooperation in criminal matters shall include facilitating and accelerating cooperation between competent ministries and judicial or equivalent authorities of the Member States in relation to proceedings and the enforcement of decisions. Such cooperation implies the necessity of the processing of relevant information subject to appropriate provisions on the protection of personal data;

(3) Legislation under Title VI of the Treaty on European Union must foster police and judicial cooperation in criminal matters with regard to its efficiency as well as its legitimacy and compliance with fundamental rights, in particular the right to protection of personal data. Common standards regarding the processing and protection of personal data processed for the purpose of preventing and combating crime can contribute to achieving both aims.

(4) The Action Plan of the Council and the Commission on how best to implement the provisions of the Treaty of Amsterdam on an area of freedom, security and justice [17] stipulated that - with regard to horizontal problems in the context of police and judicial cooperation in criminal matters - the possibilities for harmonised rules on data protection should be examined within two years from the entry into force of the Treaty. Subsequent efforts ended without success as finally no agreement could be achieved on a Draft Resolution on the personal protection rules in instruments under the third pillar of the European Union.[18]

(5) The Hague Programme on strengthening freedom, security and justice in the European Union, adopted by the European Council on 4 November 2004,[19] stresses the need for an innovative approach to the cross-border exchange of law-enforcement information. The Commission is invited to submit proposals in this regard by the end of 2005 at the latest The relevant content of the Hague Program is also reflected in the Partnership for European renewal in the field of Freedom, Security and Justice[20] and in the Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union[21] adopted on 2 June 2005. [22]

(6) The European Parliament recommended harmonising existing rules on the protection of personal data in the instruments of the current third pillar guaranteeing the same level of data protection as provided for under the first pillar.[23] The Data Protection Authorities of all Member States of the European Union and the European Data Protection Supervisor recommended a new legal instrument for data protection in the third pillar.[24]

The proposed Framework Decision on the exchange of information under the principle of availability. will fundamentally change the exchange of information between the Member States. Such development will affect personal data and the right to data protection.The implementation of the principle of availability needs to be appropriately supplemented by rules on data processing and to be counterbalanced by provisions in the area of data protection. Existing instruments at the European level do not comply with these requirements. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.;

(7) Binding rules regarding the processing and protection of personal data processed for the purpose of preventing and combating crime must supplement and support the

17 OJ C 19, 23.1.1999, p. 1

18 Council Working Document 6316/2/01 REV 2 JAI 13

19 OJ C 53, 3.3.2005, p. 1

20 COM(2005) 184 final, Brussels, 10.5.2005

21 Council Working Document 9778/2/05 REV 2 JAI 207

22 Council Working Document 11158/1/05 REV 1 JAI 255

23 No. 1 h of European Parliament recommendation to the European Council and the Council on the exchange of information and cooperation concerning terrorist offences (2005/2046(INI)), adopted on 7 June 2005

24 Declaration and Position paper on law enforcement and information exchange in the EU, adopted by the Spring Conference of European Data Protection Authorities, Krakow, 25 and 26 April 2005

exchange of information Provisions just addressing individual aspects of data processing and protection are not sufficient. A legal instrument providing for common standards for the processing and protection of personal data processed for the purpose of preventing and combating crime is necessary.

(8) A legal instrument on common standards for the processing and protection of personal data processed for the purpose of preventing and combating crime must be consistent with the overall policy of Union in the area of data processing and data protection. Wherever possible, taking into account the necessity of improving the efficiency of legitimate activities of the police, customs, judicial and other competent authorities, it should follow existing and proven principles, notably those laid down in Directive 95/46/EC or relating to the exchange of information through Europol, Eurojust, the Customs Information System or other comparable acts;

(9) The approximation of Member States' laws must not result in any lessening of the data protection they afford but must, on the contrary, seek to ensure a high level of protection in the Union.

(10) A legal instrument complying with these requirements should be largely inspired by existing definitions at EU level. The legal instrument should include: provisions on the lawfulness of processing of personal data in order to ensure that any information that might be exchanged has been processed legitimately and in accordance with fundamental principles relating to data quality taking into account the necessity of not undermining legitimate activities of the police, customs, judicial and other competent authorities; provisions laying down the conditions for transmitting and making available personal data to the competent authorities of other Member States; provisions laying down the conditions for further processing of personal data received from or made available by the competent authority of another Member State, in particular for further transmitting such data, including their transmission to competent authorities in third countries or to international bodies; provisions that are likely to have an effect on the lawfulness and quality of personal data that have been or could be made available to competent authorities in other Member States, including provisions regarding the rights of the data subject, confidentiality and security of processing, judicial remedies, liability and sanctions, the role of independent supervisory authorities and coordinated advice that may be needed at European level.

(11) It is appropriate to provide rules in accordance with recital 7 where Member States exchange information by granting each other direct automated access to their data bases.

(12) The processing and protection of personal data in the exchange of information by Europol, Eurojust and the Customs Information System is comprehensively covered in specific legal instruments.[25]

25 Europol Convention of 1995 (OJ C 316, 27.11.1995, p. 2) and, inter alia, the Rules governing the transmission of personal data by Europol to third States and third bodies (OJ C 88, 30.3.1999, p. 1),
Convention implementing the Schengen Agreement of 1990 including specific data protection provisions applicable to the Schengen Information System (OJ L 239 , 22.9.2000, p. 19), Decision setting up Eurojust of 2002 (OJ L 63, 6.3.2002, p. 1) and the Rules of procedure on the processing and protection of personal data at Eurojust (OJ C 68, 19.3.2005, p.1), Convention implementing the Schengen Agreement of 1990 including specific data protection provisions applicable to the Schengen Information System (OJ L 239 , 22.9.2000, p. 19), Convention on the use of information technology for customs purposes of 1995, including personal data protection provisions applicable to the Customs Information System (OJ C 316, 27.11.1995, p. 34). With regard to Schengen Information System particular attention has to be paid to the establishment, operation and use of the second generation Schengen information system (SIS II).

(13) It is appropriate that this Framework Decision applies to personal data which are processed in the framework of the second generation of the Schengen Information System and the related exchange of supplementary information Decision JHA/2006 …. on the establishment, operation and use of the second generation Schengen information system further supplements or clarified the principles set out in this Framework Decision where necessary.

(14) Article 47 of the Treaty on the European Union provides that nothing in this Treaty shall affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them. Accordingly, this Framework Decision does not affect the protection of personal data under Community law, in particular, under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

(15) Since the objectives of the action to be taken cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and effects of the action, be better achieved at the level of the European Union, the Council may adopt measures in accordance with the principle of subsidiarity, as set out in Article 5 of the EC Treaty and referred to in Article 2 of the EU Treaty. In accordance with the principle of proportionality as set out in Article 5 of the EC Treaty, this Framework Decision does not go beyond what is necessary to achieve those objectives.

(16) The Framework Decision respects the fundamental rights and principles recognized by the Treaty, in particular in its Article 6 (2), and reflected in the Charter of Fundamental Rights of the European Union, in particular in its Article 8.The United Kingdom is taking part in this Framework Decision, in accordance with Article 5 of the Protocol integrating the Schengen acquis into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 8 (2) of Council Decision 2000/365/EC of 29 May 2000, concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis [26].

(17) Ireland is taking part in this Framework Decision in accordance with Article 5 of the Protocol integrating the Schengen acquis into the framework of the European Union annexed to the EU Treaty and to the EC Treaty, and Article 6 (2) of Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis[27].

(18) This Framework Decision is without prejudice to the arrangements for the United Kingdom and Ireland's partial participation in the Schengen acquis, as defined in Decision 2000/365/EC and 2002/192/EC, respectively.

(19) As regards Iceland and Norway, this Framework Decision constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis, which fall within the area

[26] OJ L 131, 1.6.2000, p. 43.
[27] OJ L 64, 7.3.2002, p. 20.

referred to in Article 1(H) of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement;

(19) As regards Switzerland, this Framework Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement signed by the European Union, the European Community and the Swiss Confederation concerning the association of the Swiss Confederation with the implementation, application and development of the Schengen *acquis* which fall within the area referred to in Article 1 (H) of Council 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement read in conjunction with Article 4 (1) of the Council Decision 2004/849/EC[28] on the signing, on behalf of the European Union, and on the provisional application of certain provisions of that Agreement.(20) This Framework Decision constitutes an act building on the Schengen acquis or otherwise related to it within the meaning of Article 3(1) of the 2003 Act of Accession, except for the Article 11 of this Framework Decision for which the provisions of Article 3(2) of the 2003 Act of Accession apply.

(21) This Framework Decision does not affect specific cooperation regimes between law enforcement authorities established under Title VI of the Treaty on the European Union. In addition, according to Article 47 of the Treaty on the European Union, that provides that nothing in the EU Treaty shall affect the Treaties establishing the European Communities or the subsequent Treaties and Acts modifying or supplementing them, this Framework Decision does not affect specific cooperation regimes between Member States authorities established under EC law.

HAS ADOPTED THIS FRAMEWORK DECISION:

CHAPTER I
OBJECT, DEFINITIONS AND SCOPE

Article 1
Object

1. This Framework Decision determines common standards to ensure the protection of individuals with regard to the processing of personal data , among others, in the course of activities of police and judicial co-operation in criminal matters provided for by Title VI of the Treaty on European Union.

LS VERSION

2. Member States shall ensure that the disclosure of personal data to the competent authorities of another Member State is neither restricted nor prohibited for reasons connected with the protection of personal data as provided for under this Framework Decision.

28 OJ L 368 of 15.12.2004, p. 26

Article 2
Definitions

For the purposes of this Framework Decision:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of the processing are determined by national law or by law under Title VI of the Treaty on European Union, the controller or the specific criteria for his nomination may be designated by national law or by law under Title VI of the Treaty on European Union;

(e) ‘processor’ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his or her wishes by which the data subject signifies his agreement to personal data relating to him being processed;

(i) ‘third countries’ shall mean countries other than the Member States of the European Union, Iceland, Norway and Switzerland;

(j) ‘international bodies or organisations’ shall mean bodies or organisations established by international agreements.

(k) 'competent authorities' shall mean police forces, customs, judicial and other competent authorities of the Member States within the meaning of Article 29 of the Treaty on European Union.

Article 3
Scope

1. This Framework Decision shall apply to the processing of personal data which form part or are intended to form part of a filing system of a competent authority regardless whether the processing of the data takes place wholly or partly by automatic means or other than by automatic meansfor the purpose of the prevention, investigation, detection and prosecution of criminal offences.

2. This Framework Decision is without prejudice to the established rules for the processing of personal data

   – by the European Police Office (Europol),

   – by the European Judicial Cooperation Unit (Eurojust),

   – by the Customs Information System as set up according to the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, and any amendments made thereto.

3.

4. This Framework Decision is without prejudice to the protection of personal data under Community law, in particular under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

CHAPTER II
GENERAL RULES ON THE LAWFULNESS OF PROCESSING OF PERSONAL DATA

Article 4
Principles relating to quality of data processing

1. Member States shall provide that personal data must be:

   (a) processed fairly and lawfully;

   (b) collected for specified, explicit and legitimate purposes and not processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

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

(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 thata 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.

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with.

3. Member States shall provide that any derogation from the principles set out in paragraph 1 is prohibited unless such derogation exceptionally is provided for by law and constitutes a necessary measure to safeguard the prevention, investigation, detection and prosecution of criminal offences.

4. Member States shall provide for a clear distinction between personal data of

- a person who is suspected of having committed or having taken part in a criminal offence or who has been convicted of such an offence,
- a person who there are serious grounds for believing will commit a criminal offence,
- a person who might be called on to testify in investigations in connection with criminal offences or subsequent criminal proceedings,
- a person who has been the victim of a criminal offence or with regard to whom certain facts give reasons for believing that they could be the victims of a criminal offence,
- a person who can provide information on criminal offences, and
- a contact or associate to one of the persons mentioned above,

5. Member States shall provide that processing is only necessary if

- there are, based on specific facts, reasonable grounds to believe that the data concerned would make possible, facilitate or accelerate the prevention, investigation, detection or prosecution of a criminal offence,
- 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.

Article 5
Criteria for making data processing legitimate

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.

Article 6
Processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.

2. Paragraph 1 shall not apply where processing is

   - provided for by a law and
   - if 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.

3. Where paragraph 1 does not apply Member States shall provide for specific safeguards, for example access to the data concerned only for personnel that is responsible for the fulfilment of the legitimate task that justifies the processing according to paragraph 2.

CHAPTER III – Specific Forms of Processing

SECTION I – COLLECTION AND STORAGE

Article 7
Time limits for the storage of personal data

Member States shall provide that personal data shall be stored for no longer than necessary for the purpose of which it was collected, unless otherwise provided. Personal data of persons referred to in Article 4 (5) last indent shall be stored for only as long as is absolutely necessary for the purpose of the processing.

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.

SECTION II – TRANSMISSION AND MAKING AVAILABLE PERSONAL DATA TO THE COMPETENT AUTHORITIES OF OTHER MEMBER STATES

Article 8
Transmission and making available personal data to the competent authorities of other Member States

1. 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 the legitimate task of the transmitting or receiving authority and for the purpose of the prevention, investigation, detection or prosecution of criminal offences.

2. Member States shall provide that the transmission and making availablepersonal data to the competent authority in another Member State shall not be refused for reasons of data protection .

Article 9
Verification of quality of data that are transmitted or made available

1. Member States shall provide that the quality of personal data is verified at the latest before they are transmitted or made available. As far as possible, in all transmissions of data, judicial decisions as well as decisions not to prosecute should be indicated and data based on opinions or personal assessments checked at source before being transmitted and their degree of accuracy or reliability indicated.

2. Member States shall provide that the quality of personal data, which are made available by direct automated access to the competent authorities of other Member States, are regularly verified in order to ensure that accurate and updated data are accessed.

3. Member States shall provide that personal data which are no longer up to date or accurate shall not be transmitted.

4. Member States shall provide that a competent authority that transmitted or made available personal data to a competent authority of another Member States shall inform the latter immediately if it should establish, either on its own initiative or further to a request by the data subject that the data concerned should not have been transmitted or made available or that inaccurate or outdated data were transmitted or made available.

5. Member States shall provide that a competent authority that has been informed according to paragraph 4 shall delete or rectify the data concerned. Furthermore, that authority shall rectify the data concerned if it detects that these data are inaccurate. If that authority has reasonable grounds to believe that received personal data are inaccurate or to be deleted, it shall inform without delay the competent authority that transmitted or made available the data concerned.

6. Member States shall 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. This paragraph shall not apply if the marking of the personal data prejudices the specific action to be taken by the competent authorities and imposed by specific legislation under Title VI of the Treaty on European Union.

7. Member States shall provide that personal data received from the authority of another Member State are deleted

   – if these data should not have been transmitted, made available or received,

   – after a time limit laid down in the law of the other Member State if the authority that transmitted or made available the data concerned has informed the receiving authority of such time limit when the data concerned were transmitted or made available and unless the conditions set out in the third indent of this paragraph continue to exist,

   – if these data are not or no longer necessary for the purpose they were transmitted or made available for; if personal data were transmitted without request the receiving authority shall verify without delay if these data are necessary for the purpose they were transmitted for;

   Personal data shall not be deleted but blocked in accordance with national law if there are reasonable grounds to believe that the deletion could affect the interest of the data subject worthy of protection. Blocked data shall only be used or transmitted for the purpose they were not deleted for.

Article 10
Logging and documentation

1. Member State 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.

2. Member State 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, 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. The authority that has 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 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.

SECTION III – FURTHER PROCESSING, IN PARTICULAR FURTHER TRANSMISSION AND TRANSFER, OF DATA RECEIVED FROM OR MADE AVAILABLE BY THE COMPETENT AUTHORITIES OF OTHER MEMBER STATES

Article 11
Further processing of personal data received from or made available by the competent authority of another Member State

1. Member States shall provide that personal data received from or made available by the authority of another Member State are further processed in accordance with this Framework Decision, in particular its Articles 4, 5 and 6.

2. Member States shall provide that personal data transmitted or made available by the competent authority of another Member State may only be further processed

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

   (b) for the purpose of the prevention, investigation, detection or prosecution of serious criminal offences or for the purpose of the prevention of serious threats to public security or to a person.

3. The personal data concerned shall be further processed for the purposes referred to in paragraph 2 (b) of this article only with the prior consent of the authority that transmitted or made available the personal data.

4. Paragraph 2 (b) shall not apply if specific legislation under Title VI of the Treaty on European Union explicitly stipulates that personal data transmitted or made available by the competent authority of another Member State shall only be further processed for the purposes they were transmitted or made available for.

Article 12
Transmission to other competent authorities

Member States shall provide that personal data received from or made available by the competent authority of another Member State are further transmitted to other competent authorities of a Member State only if all of the following preconditions are met.

(a) The transmission is provided for by law clearly obliging to or authorising it..

(b) The transmission is necessary for the fulfilment of the legitimate task of the authority that has received the data concerned or of the authority to which they shall be further transmitted.

(c) The transmission is necessary for the specific purpose they were transmitted or made available for or for the purpose of the prevention, investigation, detection or

prosecution of serious criminal offences or for the purpose of the prevention of serious threats to public security or to a person.

(d) The competent authority of othe Member State that has transmitted or made available the data concerned to the competent authority that intends to further transmit them has given its consent to their further transmission.

Article 13
Transmission to authorities other than those referred to in Article 3 (1)

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 those referred to in Article 3 (1), of a Member State only in particular cases and if all of the following preconditions are met.

(a) The transmission is provided for by law clearly obliging to or authorising it.

(b) The transmission is

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 serious criminal offences or for the purpose of the prevention of serious threats to public security or to a person,

or

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

or

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

(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 consent to their further transmission.

Article 14
Transmission to private parties

Member States shall provide that personal data received from or made available by the competent authority of another Member State are further transmitted to private parties in a Member State only in particular cases and if all of the following preconditions are met.

(a) The transmission is provided for by law clearly obliging to or authorising it.

(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 serious criminal offences or for the purpose of the prevention of serious threats to public security or to a person,

(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 explicit consent in advance to their further transmission to private parties.

Article 15

Transfer to competent authorities in third countries or to international bodies

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 all the following preconditions are met.

(a) The transfer is provided for by national or international law clearly obliging to or authorising it.

(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 serious criminal offences or for the purpose of the prevention of serious threats to public security or to a person,

(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 explicit consent to their further transfer.

(d) An adequate level of data protection is ensured in the third country or by the international body to which the data concerned shall be transferred.

2. Member States shall provide that the adequacy of the level of protection afforded by a third country or international body shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment will result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer.

3. 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. If there are reasonable grounds to believe that personal data are transferred to a third country or to an international body that does not ensure an adequate level of protection within the meaning of paragraph 2, for example because of diverging positions of the Member States in that regard, the Commission shall report to the Council and, if appropriate, submit proposals to ensure a consistency and compliance with this Article.

4. 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 person.

.

Article 16
Exceptions from Articles 15, 16, 17, and 18

Articles 15, 16, 17, and 18 shall not apply if specific legislation under Title VI of the Treaty on European Union explicitly stipulates that personal data received from or made available by the competent authority of another Member State shall not be further transmitted or only be further transmitted under more specific conditions.

Article 17
Information on request of the competent authority

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

CHAPTER IV
RIGHTS OF THE DATA SUBJECT

Article 18
Right of information in cases of collection of data from the data subject with his/her knowledge

1. Member States shall provide that the controller or his representative must provide a data subject from whom data relating to him- or herself are collected with his/her knowledge with at least the following information free of cost, except where he or she already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

– the legal basis of the processing,

– the recipients or categories of recipients of the data,

– whether replies to questions or other forms of cooperation are obligatory or voluntary, as well as the possible consequences of failure to reply or to cooperate,

– the existence of the right of access to and the right to rectify the data concerning him or her

– in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

2. The provision of the information laid down in paragraph 1 shall be refused if necessary

(a) to enable the data controller to fulfil its lawful duties properly,

(b) it is likely to prejudice ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competend authorities,

(c) to protect public security and public order in a Member State,

(d) to protect the rights and freedoms of third parties,

3. except where such considerations are overridden by the interests for fundamental rights and freedoms of the data subject.If the information referred to in paragraph 1 is refused or restricted, the data controller shall inform the data subject that he or she has the right to bring an action or a complaint before the courts of that Member State .

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 data controller shall inform the data subject that he or she has the right to bring an action or a complaint before the courts of that Member State.

Article 19

Right of information where the data have not been obtained from the data subject or have been obtained from him/her without his/her knowledge or without his/her awareness that data are being collected concerning him/her

1. Where the data have not been obtained from the data subject or have been obtained from him/her without his/her knowledge or without his/her awareness that data are being collected concerning him/her, Member States shall provide that the controller or his/her 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, except where he/she already has it or the provision of the information proves impossible or would involve a disproportionate effort:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing;

(c) any further information such as

– the legal basis of the processing,

– the categories of data concerned,

– the recipients or categories of recipients,

– the existence of the right of access to and the right to rectify the data concerning him or her

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

2. The information laid down in paragraph 1 shall be not be provided if necessary

(a) to enable the data controller to fulfil its lawful duties properly,

(b) it is likely to prejudice ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competend authorities,

(c) to protect public security and public order in a Member State,

(d) to protect the rights and freedoms of third parties,

except where such considerations are overridden by the interests for fundamental rights and freedoms of the data subject.

Article 20
Right of access, rectification, erasure or blocking

1. Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

– confirmation as to whether or not data relating to him/her are being processed and information at least as to the purposes of the processing, the categories of data concerned, the legal basis of the processing and the recipients or categories of recipients to whom the data are disclosed,

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

– knowledge of the logic involved in any automatic processing of data concerning him/her at least in the case of a decision which produces legal effects concerning him/her or significantly affects him/her and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him/her;

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Framework Decision, in particular because of the incomplete or inaccurate nature of the data;

(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.

2. Any act the data subject is entitled to according to paragraph 1 shall be refused if necessary

(a) to enable the data controller to fulfil its lawful duties properly,

(b) it is likely to prejudice ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competend authorities,

(c) to protect public security and public order in a Member State,

(d) to protect the rights and freedoms of third parties,

except where such considerations are overridden by the interests for fundamental rights and freedoms of the data subject.

3. A refusal or restriction of the rights referred to in paragraph 1 shall be reasoned in writing. If the right referred to in paragraph 1 is refused or restricted, the data controller shall inform the data subject that he or she has the right to bring an action or a complaint before the courts of that Member State.

4. The reasons for a refusal according to paragraph 2 shall not be given to the data subject if their communication prejudices the purpose of the refusal. In such case the data controller shall inform the data subject that he or she has the right to bring an action or a complaint before the courts of that Member State.

Article 21
Information to third parties following rectification, blocking or erasure

Member States shall provide that appropriate technical measures are taken to ensure that, in the cases where the data controller rectifies, blocks or erases personal data following a request, a list of the suppliers and addressees of these data is automatically produced. The controller shall ensure that those included in the list are informed of the changes performed on the personal data.

CHAPTER V
Confidentiality and security of processing; notification

Article 22
Confidentiality

Any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller, unless he/she is required to do so by law. All persons called upon to work with or within a competent authority of a Member State shall be bound by strict confidentiality rules.

Article 23
Security

1. Member States shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission over a network or the making available by granting direct automated access, and against all other unlawful forms of processing, taking into account in particular the risks represented by the processing and the nature of the data to be protected.

   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 only be necessary where the effort they involve is proportionate to the objective they are designed to achieve in terms of protection.

2. In respect of automated data processing each Member State shall implement measures designed to:

   (a) deny unauthorized persons access to data processing equipment used for processing personal data (equipment access control);

   (b) prevent the unauthorized reading, copying, modification or removal of data media (data media control);

   (c) prevent the unauthorized input of data and the unauthorized inspection, modification or deletion of stored personal data (storage control);

   (d) prevent the use of automated data processing systems by unauthorized persons using data communication equipment (user control);

   (e) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

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

   (g) ensure that installed systems may, in case of interruption, be immediately restored (recovery),

   (h) ensure that the functions of the system perform without fault, that the appearance of faults in the functions is immediately reported (reliability) and that stored data cannot be corrupted by means of a malfunctioning of the system (integrity).

3. Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the

technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

4. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:

   – the processor shall act only on instructions from the controller,

   – the obligations set out in paragraph 1 and 2, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

5. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

Article 24
Register and Notification

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

   (a) the name and address of the controller and of his representative, if any;

   (b) the purpose or purposes of the processing;

   (c) a description of the category or categories of data subject and of the data or categories of data relating to them;

   (d) the legal basis of the processing operation for which the data are intended;

   (e) the recipients or categories of recipient to whom the data might be disclosed;

   (f) proposed transfers of data to third countries;

   (g) a general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 24 to ensure security of processing.

2. Member States shall specify the conditions and procedures under which information referred to in paragraph 1 must be notified to the supervisory authority.

Article 25
Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof.

2. Such prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official, who, in cases of doubt, must consult the supervisory authority.

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.

CHAPTER VI
JUDICIAL REMEDIES AND LIABILITY

Article 26
Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 31, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed to him/her by the national law applicable.

Article 27
Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Framework Decision is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage. However, a competent authority that received personal data from the competent authority of another Member State may not plead that the latter transmitted or made available inaccurate data, in order to avoid its liability vis-à-vis an injured party; if damages are awarded against the receiving authority because of its use of inaccurate data transmitted or made available by the competent authority of another Member State, the latter shall refund in full to the data controller the amount paid in damages.

.

Article 28
Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Framework Decision and shall in particular lay down effective, proportionate and dissuasive sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Framework Decision.

The powers and decisions of the supervisory authority shall not apply in the framework of criminal judicial proceedings.

CHAPTER VII
SUPERVISORY AUTHORITY AND 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

Article 29
Supervisory authority

1. Each Member State shall provide that one or more public authorities are responsible for 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.

2. Each Member State shall provide 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.

3. Each authority shall in particular be endowed with:

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

   – effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 26, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

   – the power to engage in legal proceedings where the national provisions adopted pursuant to this Framework Decision have been violated or to bring these violations to the attention of the judicial authorities.

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

4. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and freedoms in regard to the processing of personal data. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

7. The supervisory authorities shall cooperate with one another as well as with the supervisory bodies set up under Title VI of the Treaty on European Union and the European Data Protection Supervisor to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

8. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 30
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

1. 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, hereinafter referred to as 'the Working Party', is hereby set up. It shall have advisory status and act independently.

2. 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 European Data Protection Supervisor, and of a representative of the Commission.

   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. The same shall apply to the authorities established for Community institutions and bodies.

   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. The supervisory authority or authorities designated by Iceland, Norway and Switzerland shall be entitled to be represented in meetings of the Working Party insofar as issues related to the Schengen Acquis are concerned.

3. The Working Party shall adopt its opinions by a simple majority of the representatives of the supervisory authorities of the Member States.

4. The Working Party shall elect its chairperson. The chairperson's term of office shall be two years. His/her appointment shall be renewable.

5. The Working Party's secretariat shall be provided by the Commission.

6. The Working Party shall adopt its own rules of procedure.

7. The Working Party shall consider items placed on its agenda by its chairperson, either on his/her own initiative or at the request of a representative of the supervisory authorities, the Commission, the European Data Protection Supervisor or the chairpersons of the joint supervisory bodies.

Article 31

1. The Working Party shall,

   (a) examine any question covering the application of the national measures adopted under this Framework Decision in order to contribute to the uniform application of such measures,

   (b) give an opinion on the level of protection in the Member States and in third countries, in particular in order to guarantee that personal data are transferred in compliance with Article 18 of the Framework Decision to third countries or international bodies that ensure an adequate level of data protection,

   (c) advise the Commission and the 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 any other proposed measures affecting such rights and freedoms.

2. If the Working Party finds that divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the European Union are arising between the laws and practices of Member States it shall inform the Council and the Commission.

3. The Working Party may, on its own initiative, make recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the European Union for the purpose of the prevention, investigation, detection and prosecution of criminal offences.

4. The Working Party's opinions and recommendations shall be forwarded to the Council, to the Commission and to the European Parliament.

5. The Commission shall, based on information provided by the Member States, inform the Working Party of the action taken in response to its opinions and recommendations. It shall do so in a report which shall also be forwarded to the European Parliament and the Council. The report shall be made public.

6. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal

offences in the Union and in third countries, which it shall transmit to Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VIII
Final provisions

Article 32
Provisions relating to the Schengen acquis

The provisions of Articles 126 to 130 of the Convention implementing the Schengen Agreement of 14 June 1985 shall be replaced.

Article 33
Relation to existing instruments that concern the processing and protection of personal in the context of police and judicial cooperation in criminal matters

1. Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000 shall be repealed.[29]

2. Article 2 (3), first sentence, of Council Decision of 25 April 2002[30] concerning security in connection with football matches with an international dimension shall be repealed.

Article 34
Implementation

1. Member States shall take the necessary measures to comply with this Framework Decision by 1 2007.

2. By the same date 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, as well as the designation of the supervisory authority or authorities referred to in Article 31. On the basis of this information and a written report from the Commission, the Council shall before 31 December 2007 assess the extent to which Member States have taken the measures necessary to comply with this Framework Decision.

29 OJ C 197, 12.7.2000, p. 1

30 OJ L 121? 8.5.2002, p. 1

Article 35
Entry into force

This Framework Decision shall enter into force on the day of its publication in the Official Journal of the European Union.

Done at Brussels, […]

For the Council
The President
[…]