COUNCIL OF THE EUROPEAN UNION

Brussels, 13 March 2007 (15.03)
(OR. de)

7315/07

Interinstitutional File: 2005/0202 (CNS)

LIMITE

CRIMORG 53
DROIPEN 18
ENFOPOL 45
DATAPROTECT 10
COMIX 267

NOTE

from :	Presidency
to :	delegations
Nos prev. docs :	13246/06 CRIMORG 143 DROIPEN 61 ENFOPOL 161 DATAPROTECT 33 COMIX 780 5435/07 CRIMORG 12 DROIPEN 4 ENFOPOL 5 DATAPROTECT 3 ENFOCUSTOM 9 COMIX 57
Subject :	Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

1. 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.
On 13 December 2005, the Council consulted the Parliament on the proposal. The Parliament delivered its opinion on 27 September 2006. The European Data Protection Supervisor has also delivered his opinion[1] on the proposal, which he presented to the Multidisciplinary Group on Organised Crime (MDG)-Mixed Committee on 12 January 2006. On 24 January 2006, the Conference of European Data Protection Authorities also delivered an opinion[2] on the proposal.

[1] 16050/05 CRIMORG 160 DROIPEN 64 ENFOPOL 185 DATAPROTECT 8 COMIX 864.
[2] 6329/06 CRIMORG 28 DROIPEN 12 ENFOPOL 26 DATAPROTECT 4 COMIX 156.

2. 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 the meeting of the Article 36 Committee on 25 and 26 January 2007, the Presidency set out a series of basic points[3] for revising the proposal, with the aim of removing outstanding reservations and making a real improvement in third-pillar data protection. The attached Presidency revised draft reflects those points.

3. 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.

4. The attached draft is to be submitted to the Article 36 Committee at its meeting on 22 and 23 March 2007. The first reading by the MDG is scheduled for 29 and 30 March 2007.

---

[3] 5435/07 CRIMORG 12 DROIPEN 4 ENFOPOL 5 DATAPROTECT 3 ENFOCUSTOM 9 COMIX 57.

ANNEX

COUNCIL FRAMEWORK DECISION

of ....

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

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,[4]

Having regard to the opinion of the European Parliament,[5]

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.

(2) Common action in the field of police cooperation under Article 30(1)(b) of the Treaty on European Union and common action on judicial cooperation in criminal matters under Article 31(1)(a) of the Treaty on European Union imply the necessity of the processing of relevant information which should be subject to appropriate provisions on the protection of personal data.

---

4 …

5 …

(3) Legislation falling within the ambit of Title VI of the Treaty on European Union should 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 privacy and 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 Hague Programme on strengthening freedom, security and justice in the European Union, adopted by the European Council on 4 November 2004, stressed the need for an innovative approach to the cross-border exchange of law-enforcement information under strict observation of key conditions in the area of data protection and invited the Commission to submit proposals in this regard by the end of 2005 at the latest. This was reflected in the *Council and Commission Action Plan implementing the Hague Programme on strengthening freedom, security and justice in the European Union*[6].

(5) The exchange of personal data in the framework of police and judicial cooperation in criminal matters, notably under the principle of availability of information as laid down in the Hague Programme, should be supported by clear binding rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way excluding any obstruction of this cooperation between the Member States while fully respecting fundamental rights of individuals. Existing instruments at the European level do not suffice. 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] 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 Title VI of the Treaty on European Union, or, in any case, to processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.

---

[6] OJ C 198, 12.8.2005, p. 1.
[7] OJ L 281, 23.11.1995, p. 31.

(5a) The 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. (…)

(5b) (…)

(6) A legal instrument on common standards for the protection of personal data processed for the purpose of preventing and combating crime should be consistent with the overall policy of the European Union in the area of privacy 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 therefore follow existing and proven principles and definitions, notably those laid down in Directive 95/46/EC of the European Parliament and of the Council relating to the exchange of information by Europol, Eurojust, or processed via the Customs Information System or other comparable instruments.

(6a) Member States will also apply 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.

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

(8) It is necessary to specify the objectives of data protection in the framework of police and judicial activities and to lay down rules concerning 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. At the same time the legitimate activities of the police, customs, judicial and other competent authorities should not be jeopardised in any way.

(8a) (…)

(9) Ensuring a high level of protection of the personal data of European citizens requires common provisions to determine the lawfulness and the quality of data processed by competent authorities in other Member States.

(9a) (…)

(10) It is appropriate to lay down at the European level the conditions under which competent authorities of the Member States should be allowed to transmit and make available personal data to authorities and private parties in other Member States.

(11) The further processing of personal data received from or made available by the competent authority of another Member State, in particular the further transmission of or making available such data, should be subject to common rules at European level.

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

(13) It may be necessary to inform data subjects regarding the processing of their data, in particular where there has been particularly serious encroachment on their rights as a result of secret data collection measures, in order to ensure that data subjects can have effective legal protection.

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

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

(15a) This Framework Decision allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Framework Decision.

(16) The establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of personal data processed in the framework of police and judicial cooperation between the Member States.

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

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

(19) Article 47 of the Treaty on European Union stipulates that none of its provisions 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 as provided for in Directive 95/46/EC of the European Parliament and of the Council , in Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data[8] and in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)[9].

---

[8] OJ L 8, 12.1.2001, p. 1.

[9] OJ L 201, 31.7.2001, p. 37.

(20) Improving data protection within the third pillar depends on the Framework Decision covering the whole of the third pillar, including Europol, Eurojust and the third-pillar Customs Information System. Care must be taken to ensure that more extensive specific data protection rules in the relevant legal instruments remain unaffected. Where the Framework Decision is to replace existing specific data protection provisions, the Data Protection Framework Decision stipulates this explicitly.

(21) The provisions regarding the protection of personal data, laid down in Title IV of the Convention of 1990 implementing the Schengen Agreement of 14 June 1985 on the gradual abolition of checks at the common borders[10] (hereinafter referred to as the "Schengen Convention") and integrated into the framework of the European Union pursuant to the Protocol annexed to the Treaty on European Union and the Treaty establishing the European Community, should be replaced by the relevant rules of this Framework Decision for the purposes of matters falling within the scope of the Treaty on European Union.

(21a) References to provisions in national law regarding legal instruments adopted pursuant to Title VI of the Treaty on European Union are to be construed as meaning that the corresponding implementing rules are to be found in the relevant legal instruments themselves and not in national legislation.

(22) It is appropriate that this Framework Decision also applies to the personal data which are processed in the framework of the second generation of the Schengen Information System and the related exchange of supplementary information pursuant to Decision JHA/2006/ … on the establishment, operation and use of the second generation Schengen Information System.

[10] OJ L 239, 22.9.2000, p. 19.

(23) This Framework Decision is without prejudice to the rules pertaining to illicit access to data laid down in the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[11].

(24) It is appropriate to replace Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[12].

(25) This Framework Decision does not affect the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. (…).

(26) Since the objectives of the action to be taken, namely the determination of common rules for the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, cannot be sufficiently achieved by the Member States acting alone, 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 also in Article 5 of the EC Treaty, this Framework Decision does not go beyond what is necessary to achieve those objectives.

(27) 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 [13].

---

11 OJ L 69, 16.3.2005, p. 67.
12 OJ C 197, 12.7.2000, p. 3.
13 OJ L 131, 1.6.2000, p. 43.

(28) 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.

(29) 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 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[14].

(30) 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 Decision 1999/437/EC of 17 May 1999 read in conjunction with Article 4(1) of the Council Decision 2004/849/EC on the signing, on behalf of the European Union, and on the provisional application of certain provisions of that Agreement[15].

(31) 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.

---

[14] OJ L 176, 10.7.1999, p. 31.
[15] OJ L 368, 15.12.2004, p. 26.

(32) This Framework Decision respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. This Framework Decision seeks to ensure full respect for the rights to privacy and the protection of personal data in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union,

HAS ADOPTED THIS FRAMEWORK DECISION:

CHAPTER I
OBJECT, DEFINITIONS AND SCOPE

Article 1

Purpose and scope

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

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

3. This Framework Decision shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means, of personal data which form part of a filing system or are intended to form part of a filing system.

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

5. This Framework Decision shall not preclude the Council and Member States from providing safeguards for the protection of personal data (…) higher than those established in this Framework Decision. Such existing or future safeguards shall take precedence over this Framework Decision. Member States shall, however, ensure that data transmissions to other Member States or to Community institutions or bodies shall not be subjected to higher safeguards than similar national data transmissions.

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, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

(c) "blocking" shall mean the marking of stored personal data with the aim of limiting their processing in future;

(d) "personal data filing system" ("filing system") shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

(e) "processor" shall mean any body which processes personal data on behalf of the controller;

(f) "recipient" shall mean any (…) body to which data are disclosed (…);

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

(h) "international bodies" shall mean bodies or organisations established by international agreements or declared as an international body;

(i) "competent authorities" shall mean institutions and bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union as well as police, customs, judicial and other competent authorities of the Member States that are authorised by national law to process personal data within the scope of this Framework Decision and are responsible therefor; a competent authority shall be responsible where it alone or jointly with others determines the purposes and means of the processing of personal data or where responsibility is established by national legal provisions or legal provisions enacted in accordance with Title VI of the Treaty on European Union;

(j) "marking" shall mean the marking of stored personal data without the aim of limiting their processing in future;

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

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF PROCESSING OF PERSONAL DATA

Article 3

Principles of lawfulness, proportionality and purpose

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

2. Further processing for another purpose shall be permitted insofar as:

(a) it is compatible with the purpose for which the data were collected,

(b) the competent authorities collect the data in accordance with the legal provisions applicable to that purpose and

(c) processing is essential and appropriate to that purpose.

Article 4

Correction requirement

Personal data shall be corrected if inaccurate and, where necessary, updated.

Article 5

Erasure and blocking

1. Personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully processed further.

2. Personal data shall be blocked instead of erased if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose they were not erased for.

Article 6

Establishment of time-limits for erasure and review

Appropriate time-limits shall be established for the erasure of personal data or for a periodic review of the need for the storage. Procedural measures shall ensure that these are observed.

Article 7

Processing of special categories of data

(…) The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life shall be permitted only when this is strictly necessary and when suitable additional safeguards are provided.

Article 8

Automated individual decisions

A decision which produces an adverse legal effect for the data subject or seriously affects him and which is based solely on automated data processing for the purposes of assessing individual aspects of the data subject shall be permitted only when the legitimate interests of the data subject are safeguarded by law.

CHAPTER III

TRANSMISSION OF AND MAKING AVAILABLE PERSONAL DATA TO THE COMPETENT AUTHORITIES OF OTHER MEMBER STATES OR INSTITUTIONS AND BODIES ESTABLISHED ON THE BASIS OF COUNCIL ACTS PURSUANT TO TITLE VI OF THE TREATY ON EUROPEAN UNION

Article 9

Verification of quality of data that are transmitted or made available

1. The competent authorities shall take all reasonable steps to provide that personal data which are no longer accurate or up to date are not transmitted or made available. To that end, the competent authorities shall, as far as practicable, verify the quality of personal data (..) before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy or reliability.

2. If personal data were transmitted without request the receiving authority shall verify without delay whether these data are necessary for the purpose for which they were transmitted.

3. If it emerges that incorrect data, or data which should not have been transmitted, have been transmitted, the recipient must be notified without delay. The data must be corrected or erased without delay.

(…)

Article 10

Compliance with time-limits for erasure and review

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

2. The data may be blocked instead of erased when the requirements of Article 5(2) are met.

Article 11

Logging and documentation

1. All transmissions of personal data are to be logged or documented for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security.

2. Data under paragraph 1 shall be communicated on request to the competent supervisory authority for the control of data protection. The competent supervisory authority shall use this information only for the control of data protection and for ensuring proper data processing as well as data integrity and security.

3.

Article 12

Purpose of personal data received from or made available by another Member State

1. (…) Personal data received from or made available by the competent authority of another Member State may be further processed only for the following purposes other than those for which they were transmitted (…):

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

   (b) other judicial and administrative proceedings directly related to purposes referred to in Article 3(1);

   (c) the prevention of an immediate and serious threat to public security; or

   (d) any other purpose only with the prior consent of the competent authority that has transmitted or made available the personal data, unless the competent authority concerned has obtained the consent of the data subject,

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

2. In cases where appropriate conditions are laid down for the processing of personal data on the basis of Council acts in accordance with Title VI of the Treaty on European Union, these conditions shall take precedence over paragraph 1.

3. This Article shall not apply to personal data which a Member State has obtained within the scope of this Framework Decision and which originate in that Member State.

Article 13

Compliance with national processing restrictions

The transmitting authority shall inform the recipient of processing restrictions applicable under its national law to data exchanges between competent authorities within that Member State. The recipient must also comply with these processing restrictions.

Article 14

Transfer to competent authorities in third States or to international bodies

Personal data received from or made available by the competent authority of another Member State may be transferred to third States or international bodies only if the competent authority of the Member States which transmitted the data has given its consent to transfer in compliance with its national law.

Article 15

Information on request of the competent authority

The recipient shall inform the competent authority which transmitted or made available the personal data about their use and further processing.

CHAPTER IV
RIGHTS OF THE DATA SUBJECT

Article 16

Information

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

Article 17

Access

1. Every data subject shall receive from the competent authority or from the body otherwise competent under national law, without constraint and without excessive delay or expense, at least the following:

   (a) confirmation as to whether or not data relating to him are being processed and information on the recipients or categories of recipients to whom the data have been disclosed;

   (b) communication of the data undergoing processing.

2. Access may be refused only if, in the particular case,

   (a) it would jeopardise the proper performance of the tasks of the competent authority;

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

(c) the data or the fact of their storage must be kept secret pursuant to a legal provision or by reason of their nature, in particular for the sake of the overriding interests of a third party;

(d) the data are only stored since, by reason of legal provisions, they may not be erased or because they serve exclusively purposes of data protection or the monitoring of data protection and the granting of access would involve disproportionate expense,

and the interest of the data subject in access must for that reason be overridden.

3. Any refusal or restriction of access shall be set out in writing to the data subject. At the same time, the factual or legal reasons on which the decision is based shall also be communicated to him. Paragraph 2(a), (b) and (c) shall apply to this communication *mutatis mutandis*. In this case the data subject shall be advised that he may appeal to the competent supervisory authority. This right of appeal shall not apply if the national law of the Member State provides for another judicial remedy against this refusal or if the information has been refused or restricted by the competent supervisory authority itself. This authority shall, when investigating the appeal, only inform the data subject whether the controller has acted correctly or not.

Article 18

Rectification, erasure or blocking

1. The data subject is entitled to expect the competent authority to fulfil its duties concerning the rectification, erasure or blocking of personal data which arise from this Framework Decision.

2. If the accuracy of an item of personal data is denied by the data subject and its accuracy or inaccuracy cannot be ascertained, that item of data shall be referenced.

Article 19

Compensation

1. (…) 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 competent authority for the damage suffered.

2. Where a competent authority of a Member State has transmitted personal data, the recipient cannot, in the context of its liability vis-à-vis the injured party in accordance with national law, cite in its defence that the data transmitted were inaccurate. If the recipient pays compensation for damage caused by the use of incorrectly transmitted data, the transmitting competent authority shall refund in full to the recipient the amount paid in damages.

3. The liability of institutions and bodies established by Council acts pursuant to Title VI of the Treaty on European Union shall be governed by the relevant provisions applying to them.

Article 20

Judicial remedies

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

CHAPTER V

Confidentiality and security of processing

Article 21

Confidentiality of processing

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

Article 22

Security of processing

1. Member States shall provide that the competent authorities must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised 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. (…)

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 unauthorised reading, copying, modification or removal of data media (data media control);

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

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

(e) ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);

(f) 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);

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

(h) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(i) ensure that installed systems may, in case of interruption, be restored (recovery);

(j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored data cannot be corrupted by means of a malfunctioning of the system (integrity).

3. Member States shall provide that processors may be designated only if they guarantee that they achieve the requisite technical and organisational measures under paragraph 1 and comply with the instructions under Article 21. The competent authority shall monitor the processor in that respect.

4. Personal data may be processed by a processor only on the basis of a legal act or a written contract.

Article 23

Prior consultation

Member States shall provide that the processing of personal data shall be subject to prior checking by the competent supervisory authority where:

(a) special categories of data under Article 7 are to be processed, or

(b) the type of processing, in particular using new forms of processing, holds exceptional risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject.

Article 24

Sanctions

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.

CHAPTER VI

(…) Data protection monitoring

Article 25

National supervisory authorities

1. Each Member State shall provide that one or more independent public authorities are responsible for advising and monitoring it in the application within its territory of the provisions it adopts pursuant to this Framework Decision and in the processing of personal data which fall within the scope of this Framework Decision.

2. Each authority shall be endowed in particular with:

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

   (b) effective powers of intervention, such as that of delivering opinions before processing operations are carried out, (…) 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;

   (c) the power to engage in legal proceedings where the national provisions adopted pursuant to this Framework Decision have been infringed or to bring such infringements to the attention of the judicial authorities. Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

3. Each supervisory authority shall hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim. (…)

4. Member States shall provide that the members and staff of the supervisory authority are also to be bound by the data protection provisions applicable to the competent authority in question and, 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 26

Joint supervisory authority

1. The observance of data protection rules in the processing of personal data by institutions or bodies established by Council acts pursuant to Title VI of the Treaty on European Union shall be supervised and monitored by an independent joint supervisory body.

2. The composition, tasks and powers of the joint supervisory authority shall be laid down by Member States through a Council Decision under Article 34(2)(c) of the Treaty on European Union. The joint supervisory authority shall in particular monitor the proper use of data-processing programs by which personal data are to be processed and advise the Commission and Member States on any proposed amendment of this Framework Decision, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences and on any other proposed measures affecting such rights and freedoms.

3. Upon entry into force of the Decision referred to in paragraph 2, the following shall be replaced:

- Article 115 of the Schengen Convention;

- Article 24 of the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention);

- Article 23 of Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime;

- Article 18 of 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.

CHAPTER VII
FINAL PROVISIONS

Article 27

Relationship to Agreements with third States

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

Article 28

Implementation

1. Member States shall take the necessary measures to comply with this Framework Decision at the latest two years after its adoption.

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 national law the obligations imposed on them under this Framework Decision, as well as information on the designation of the supervisory authority or authorities referred to in Article 25. 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.

Article 29

Entry into force

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

Done at Brussels,

For the Council

The President