COUNCIL OF THE EUROPEAN UNION

Brussels, 12 October 2007

Interinstitutional File: 2005/0202 (CNS)

11365/3/07 REV 3

LIMITE

CRIMORG 118
DROIPEN 66
ENFOPOL 130
DATAPROTECT 30
COMIX 621
ENFOCUSTOM 77

NOTE

from :	Presidency
to :	Delegations
Nos prev. doc :	12154/2/07 REV 2 CRIMORG 128 DROIPEN 79 ENFOPOL 142 DATAPROTECT 37 COMIX 708 ENFOCUSTOM 84 11365/2/07 REV 2 CRIMORG 118 DROIPEN 66 ENFOPOL 130 DATAPROTECT 30 COMIX 621 ENFOCUSTOM 77
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 General Secretariat of the Council. On 13 December 2005 the Council consulted the Parliament on the proposal. The Parliament delivered its opinion on 27 September 2006. In the meantime, the European Parliament has delivered a second opinion on the revised draft on 6 June 2007.
   The European Data Protection Supervisor has also delivered three opinions [1] on the proposal.

[1] 16050/05 CRIMORG 160 DROIPEN 64 ENFOPOL 185 DATAPROTECT 8 COMIX 864; 16015/06 CRIMORG 190 DROIPEN 73 ENFOPOL 208 DATAPROTECT 49 COMIX 1011; 11701/07 CRIMORG 124 DROIPEN 71 ENFOPOL 134 DATAPROTECT 34 ENFOCUSTOM 81 COMIX 655

2. The file was discussed at the Council meeting of 18 September 2007, at which an agreement was reached on the regime for onward transfer of personal data obtained from another Member State to third States. The Council also confirmed the understanding that the DPFD text applies to the cross-border exchange of personal data only.
   DK, IE, SE and UK have entered a parliamentary scrutiny reservation.

3. After the Commission presented its proposal to the meeting of the Multidisciplinary group on organised crime (MDG) - Mixed Committee on 9 November 2005, the file has been discussed in the Multidisciplinary group for almost two years. Following the discussions at the MDG meeting of 4 and 5 October, the Presidency deems that the remaining issues cannot be resolved at experts level, but should be resolved at Coreper level, assisted by JHA Counsellors. It is the intention of the Presidency to reach a general approach on the DPFD text at the Council meeting of 9 November 2007. This general approach will pertain solely to the provisions of the Framework Decision and not to the recitals, which will be revisited at a later stage. However, recitals 6, 6a, 12a, 12b and 25 have already been agreed by the Council.

4. Five questions have been submitted to Coreper on 11 October 2007[2]. The follow-up to the Coreper discussion is set out in 13818/07 CRIMORG 146 DROIPEN 89 ENFOPOL 166 DATAPROTECT 44 ENFOCUSTOM 99 COMIX 871.

   The Presidency invites the delegations to discuss the issues set out in 13818/07 as well as all other outstanding issues on the DPFD as indicated in the annex to this note.

---

[2] 13818/07 CRIMORG 146 DROIPEN 89 ENFOPOL 166 DATAPROTECT 44 ENFOCUSTOM 99 COMIX 871.

ANNEX I

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,[3]

Having regard to the opinion of the European Parliament,[4]

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.

---

3 …

4 …

(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* [5].

(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 [6] 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.

---

[5] OJ C 198, 12.8.2005, p. 1.
[6] 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. The Framework Decision leaves it to Member States to determine more precisely at national level which other purposes are to be considered incompatible with the purpose for which the personal data were originally collected. In general, further processing for historical, statistical or scientific purposes is not incompatible with the original purpose of the processing.

(6) The scope of the Framework Decision is limited to the processing of personal data transmitted or made available between Member States. No conclusions can be inferred from this limitation regarding the competence of the European Union to adopt acts relating to the collection and processing of personal data at national level or the expediency for the Union to do so in the future.

(6a) To facilitate data exchanges in the European Union, Member States intend to ensure that the standard of data protection achieved in national data-processing matches that provided for in this Framework Decision. With regard to national data processing, this Framework Decision does not preclude Member States from providing safeguards for the protection of personal data higher than those established in this Framework Decision.

(6b) This Framework Decision 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.

(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.

(7a) This Framework Decision is without prejudice to legislative and other regulatory measures of Member States concerning essential national security interests and specific intelligence activities in the field of national security.

(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) The principle of accuracy of data is to be applied taking account of the nature and purpose of the processing concerned. For example, in particular in judicial proceedings data are based on the subjective perception of individuals and in some cases are totally unverifiable. Consequently, the requirement of accuracy cannot appertain to the accuracy of a statement but merely to the fact that a specific statement has been made. Another consideration is that in some cases the content of filing systems - and hence the data - is partially reviewed but the data concerned may remain in the filing systems, for example for documentation purposes.

(8b) Archiving in a separate data set is permissible only if the data are no longer required and used for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Archiving in a separate data set is also permissible if the archived data are stored in a database with other data in such a way that they can no longer be used for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The appropriateness of the archiving period depends on the purposes of archiving and the legitimate interests of the data subjects. In the case of archiving for historical purposes a very long period may also be envisaged.

(8c) Data may also be erased by destroying the data medium.

(8d) As regards inaccurate, incomplete or no longer up-to-date data transmitted or made available to another Members and further processed by quasi-judicial authorities, meaning authorities with powers to make legally binding decisions, its correction, erasure or blocking shall be enforced according to national law.

(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.

(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 received from other Member States to authorities and private parties in (…) Member States. In many cases the communication of personal data by the judiciary, police or customs to private parties is necessary to prosecute crime or avert threats, for example, by issuing alerts concerning forgeries of securities to banks and credit institutions, or, in the area of vehicle crime, by communicating personal data to insurance companies in order to prevent illicit trafficking in stolen motor vehicles or to improve the conditions for the recovery of stolen motor vehicles from abroad. This is not tantamount to the transfer of police or judicial tasks to private parties.

(10a) The rules regarding the communication of personal data by the judiciary, police or customs to private parties are not concerned with the disclosure of data to private parties (such as defence lawyers and victims) in the context of criminal proceedings (...).

(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.

(11a) Where personal data may be further processed after the Member State from which the data were obtained has given its consent, each Member State may determine the modalities of such consent, including, for example, by way of general consent for categories of information or categories of further processing.

(11b) Where personal data may be further processed for administrative proceedings, these proceedings also include activities by or on behalf of regulatory and supervisory bodies, such as bodies wholly or partially responsible for regulating or supervising financial, charitable or professional matters.

(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.

(12a) Where personal data are transferred from a Member State of the European Union to third countries or international bodies, such transfer can, in principle, take place only after the Member State from which the data were obtained has given its consent to the transfer. Each Member State may determine the modalities of such consent, including, for example, by way of general consent for categories of information or for specified countries.

(12b) The interests of efficient law enforcement co-operation demand that where the nature of the threat to the public security of a Member State or a third State is so immediate as to render it impossible to obtain prior consent in good time, the competent authority may forward the relevant personal data to the third State concerned without such prior consent. The same could apply where other essential interests of a Member State of equal importance are at stake, for example where the critical infrastructure of a Member State could be the subject of an immediate and serious threat or where a Member State's financial system could be seriously disrupted.

(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.

(14a) Some Member States have ensured the right of access of the data subject in criminal matters through a system of indirect access, where the national supervisory authority, in place of the data subject, has access to all the personal data related to the data subject without any restriction and may also correct, erase or update the inaccurate data. In this case, the national law of those Member States may provide that the national supervisory authority will only inform the data subject that all the necessary verifications have taken place. However, those Member States also provide for possibilities of direct access for the data subject in specific cases, such as access to judicial records, to obtain copies of own criminal records or of own hearing by the police services[7].

(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.

(15b) When necessary to protect personal data in relation to (...) processing which by scale or by type hold exceptional risks for fundamental rights and freedoms, for example processing by means of new technologies, mechanisms or procedures, it is appropriate to ensure that the competent national supervisory authorities are consulted prior to the establishment of filing systems aimed at the processing of these data.

(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.

[7] New recital to clarify Article 17.

(16a) The authorities already established in Member States under Article 28 of Directive 95/46/EC may also assume responsibility for the tasks to be performed by the national supervisory authorities to be established under this Framework Decision.

(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, or 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, the independence of the judiciary or the specific intelligence activities in the field of national security.

(18) (….)

(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].

(20) (…)

(21) (…)

[8] OJ L 8, 12.1.2001, p. 1.
[9] OJ L 201, 31.7.2001, p. 37.

(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) (…).

(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 [10].

(24) This Framework Decision is without prejudice to existing obligations and commitments incumbent upon Member States or upon the European Union by virtue of bilateral and/or multilateral agreements with third States. Future agreements must comply with the rules on exchanges with third States.

(24a) This Framework Decision is without prejudice to specific data protection provisions in existing Council acts.

(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, the Additional Protocol to that Convention of 8 November 2001 or the Council of Europe conventions on judicial co-operation in criminal matters.

[10] OJ L 69, 16.3.2005, p. 67.

(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 [11].

(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) and (I) of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement [12].

---

[11] OJ L 131, 1.6.2000, p. 43.
[12] OJ L 176, 10.7.1999, p. 31.

(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) and (I) 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 [13].

(31)

(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.

[13] OJ L 368, 15.12.2004, p. 26.

HAS ADOPTED THIS FRAMEWORK DECISION:

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 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, for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, personal data are

   (a) transmitted or made available between Member States or from Member States to authorities or to information systems established on the basis of Council acts, or

   (b) further processed for the same purpose by the Member State which receives such data from another from another Member State or from authorities or information systems established on the basis of Council acts.

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. This Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security[14].

[14] DE reservation.

5. This Framework Decision shall not preclude Member States from providing, for the protection of personal data processed or collected[15] at national level, higher safeguards than those established in this Framework Decision.

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[16];

(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;

---

[15] CZ reservation.
[16] IT reservation.

(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)

(i) "competent authorities" shall mean authorities 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;

(j) "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. If the purposes and means of processing are established by national legal provisions or by legal provisions enacted in accordance with Title VI of the Treaty on European Union, the controller or the criteria for his appointment can be determined by national legal provisions or by legal provisions enacted in accordance with Title VI of the Treaty on European Union;

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

(l) "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[17] be attributed to an identified or identifiable individual.

[17] AT reservation.

Article 3

Principles of lawfulness, proportionality and purpose[18]

1. Personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data must be legitimate and adequate, relevant and not excessive.

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

   (a) it is not incompatible with the purpose for which the data were collected (…)[19];

   (b) the competent authorities are authorised to process such data in accordance with the legal provisions applicable; and

   (c) processing is necessary and proportionate to that purpose.

   The competent authorities may also further process 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.

Article 4

Correction, erasure and blocking [20]

1. Personal data shall be corrected if inaccurate and, where this is possible and necessary, and completed or updated.

2. 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 further processed. Archiving of those data in a separate data set for an appropriate period in accordance with national law shall not be affected by this provision.

---

18 IT reservation.
19 NL scrutiny reservation.
20 AT, DK and RO scrutiny reservation.

3. 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[21]. Blocked data shall be processed only for the purpose which prevented their erasure.

4. When the data are contained in a judicial decision or record related to the issuance of a judicial decision, the correction, erasure or blocking shall be enforced in accordance with national rules on judicial proceedings[22].

Article 5

(…)[23]

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 the domestic law provides adequate safeguards.

---

21 UK proposal to add: 'or in exceptional circumstances, the human rights of others'. AT, DE, FR, GR and NO scrutiny reservation on this proposal.

22 AT scrutiny reservation.

23 The content of Article 5 has been moved to Article 4(2) and (3).

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.

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 inaccurate, incomplete or no longer 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, completeness, up-to-dateness and reliability. 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.

2. If it emerges that incorrect data have been transmitted or data have been unlawfully transmitted, the recipient must be notified without delay. The data must be corrected, erased, or blocked without delay in accordance with Article 4.

Article 10

Time-limits

1. The transmitting authority may[24] upon transmission or making available of the data, within the (...) national law and according to Articles 5 and 6 indicate the time-limits for the retention of data, following the expiry of which the recipient must also erase or block the data or review whether or not they are still needed. The obligation to erase or block the data[25] shall not apply if, at the time of the expiry of these time-limits, the data are required for a current investigation, prosecution of crimes or enforcement of criminal penalties[26].

2. Where the transmitting authority has refrained from indicating a time-limit in accordance with paragraph 1, the time- limits in accordance with Articles 5 and 6 for the retention of data provided for under the national law of the receiving Member States shall apply[27].

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. Logs or documentation prepared 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.

---

[24] AT scrutiny reservation. AT would prefer this to be made mandatory where national law so provides, but the Presidency concurs with those delegations that think this is essentially a matter for domestic law.

[25] UK demands that words 'or for review' be added.

[26] DE deems that absolute time limits must always be respected.

[27] RO scrutiny reservation.

Article 12

Processing 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, in accordance with the requirements of Article 3(2), be further processed only for the following purposes other than those for which they were transmitted or made available:

   (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 the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

   (c) the prevention of an immediate and serious threat to public security[28]; or

   (d) any other purpose only with the prior consent of the transmitting Member State or with the consent[29] of the data subject, given in accordance with national law.

   The competent authorities may also further process 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.

[28] Scrutiny reservation by NL, linked to Article 1(4).

[29] IT scrutiny reservation: would prefer 'of required by national law'. Obviously the consent (of the Member State and of the data subject) must be given in accordance with national law. See recital 11a.

Article 13

Compliance with national processing restrictions[30]

1. Without prejudice to the rules of this Framework Decision, Member States shall not apply higher safeguards regarding data transmissions to other Member States or to authorities established pursuant to Title VI of the Treaty on European Union (…) regarding than similar national data transmissions[31].

2. Where (...), under the law of the transmitting Member State, specific processing restrictions apply in specific circumstances to data exchanges between competent authorities within that Member State, the transmitting authority shall inform the recipient of such restrictions. The recipient shall ensure that these processing restrictions are met.

Article 14

Transfer to competent authorities in third States or to international bodies

1. Member States shall provide that personal data transmitted or made available by the competent authority of another Member State may be transferred to third States or international bodies or organisations established by international agreements or declared as an international body only if

   (a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

   (b) the receiving authority in the third State or receiving international body or organisation is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

   (c) the Member State from which the data were obtained has given its consent to transfer in compliance with its national law, and

[30] Changes made pursuant to NL proposal.
[31] AT and DK scrutiny reservation.

(d) the third State or international body concerned ensures an adequate level of protection for the intended data processing.

2. Transfer without prior consent in accordance with paragraph 1, point c, shall be permissible only if transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and the prior consent cannot be obtained in good time. The authority responsible for giving consent shall be informed without delay.

3. By way of derogation from paragraph 1, point d, personal data may be transferred if

(a) the national law of the Member State transferring the data so provides for it because of
   i. legitimate specific interests of the data subject, or
   ii. legitimate prevailing interests, especially important public interests, or

(b) the third State or receiving international body or organisation provides safeguards which are deemed adequate by the Member State concerned according to its national law.

4. The adequacy of the level of protection referred to in paragraph 1, point d, shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the State of origin and the State or international organisation of final destination of the data, the rules of law, both general and sectoral, in force in the third State or international organisation in question and the professional rules and security measures which are complied with there.

Article 14a

Transmission to private parties in Member States[32]

1. Member States shall provide that personal data received from or made available by the competent authority of another Member State may be transmitted to private parties (…) only if:

   (a) the competent authority of the Member State from which the data were obtained has consented to transmission in compliance with its national law,

   (b) no legitimate specific interests of the data subject prevent transmission and

   (c) in particular cases transfer is essential for the competent authority transmitting the data to a private party for:

      (i) the performance of a task lawfully assigned to it;

      (ii) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

      (iii) the prevention of an immediate and serious threat to public security, or

      (iv) the prevention of serious harm to the rights of individuals.

2. The competent authority transmitting the data to a private party shall inform the latter of the purposes for which the data may exclusively be used.

Article 15

Information on request of the competent authority

The recipient shall, on request, inform the competent authority which transmitted or made available the personal data about their processing.

[32] Scrutiny reservations by AT and GR.

Article 16

Information for the data subject[33]

Where personal data are being or have been transmitted or made available to the competent authority of another Member State, the Member States shall ensure that (...) the data subject shall be informed of the fact that personal data are being collected, of the categories of data involved, of the controller and the purposes for which the data are being collected or further processed. This shall not apply if:

1. the provision of such information proves, in general or in the particular case, to be incompatible with the permissible purposes of the processing;

2. it involves, in general or in the particular case, a disproportionate effort compared to the legitimate interests of the data subject;

3. the data subject already has the information or may obtain it without considerable effort, especially if that information has been made available in an appropriate way.

4. (…)

Article 17

Right of access [34]

1. Every data subject is entitled, on request made at reasonable intervals, to receive (…) without constraint and without excessive delay or expense,:

   (a) at least a confirmation from the controller or from the national supervisory authority as to whether or not data relating to him have been transmitted or made available and information on the recipients or categories of recipients to whom the data have been disclosed and communication of the data undergoing processing; or

[33] Scrutiny reservations by AT, CZ, and UK. Some delegation would have preferred that this obligation be incumbent upon the receiving rather than the transmitting Member State.

[34] AT, RO, IS, IT and IE scrutiny reservations.

(b) at least a confirmation from the national supervisory authority that all necessary verifications have taken place[35].

2. The Member States may adopt legislative measures restricting access to information pursuant to paragraph 1(a), where such a restriction, with due regard for the legitimate interests of the person concerned, constitutes a necessary and proportional measure:

(a) to avoid obstructing official or legal inquiries, investigations or procedures (…);

(b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;

(c) for protecting public security;

(d) for protecting national security;

(e) for protection of the data subject or of the rights and freedoms of others.

3. [36]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. This communication may be waived where a reason pursuant to paragraph 2, points (a) to (e), exists. In all of these cases the data subject shall be advised that he may appeal to the competent national supervisory authority, a judicial authority or to a court.

[35] GR and FI scrutiny reservation.
[36] Scrutiny reservation by HU concerning paragraph 3.

Article 18

Right to rectification, erasure or blocking

1. The data subject is entitled to expect the controller to fulfil its duties in accordance with Article 4 (…) concerning the rectification, erasure or blocking of personal data which arise from this Framework Decision. Member States shall lay down whether the data subject can assert this right directly against the controller or through the intermediary of the competent national supervisory authority. If the controller refuses rectification, erasure or blocking, the refusal must be communicated in writing and the data subject informed of the possibilities provided for in national law for lodging a complaint or seeking judicial remedy. When the complaint or judicial remedy is examined, the data subject shall be informed whether the controller acted properly or not. Member States may also provide that the data subject shall only be informed by the competent national supervisory authority that a review has taken place.

2. If the accuracy of an item of personal data is denied by the data subject and its accuracy or inaccuracy cannot be ascertained, referencing of that item of data may take place. [37]

Article 19

Right to 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 controller or other authority competent under national law for the damage suffered.

[37] IT scrutiny reservation related to the question on which Member State this obligation is incumbent.

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 to the recipient the amount paid in damages, taking into account any fault that may lie with the recipient.

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 right to seek judicial remedy for any breach of the rights guaranteed to him by the applicable national law.

Article 21

Confidentiality of processing

1. Persons who have access to personal data which fall within the scope of this Framework Decision may process such data only as members or on the instructions of the competent authority, unless there are legal obligations to do so.

2. 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 unauthorised 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 unauthorised 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 ensure that the competent national supervisory authorities are consulted prior to the processing of (…) personal data which will form part of a new filing system to be created to be created where:

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

(b) the form of processing, in particular using new forms of processing, holds otherwise 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.

Article 25

National supervisory authorities [38]

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

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, for example, 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.

[38] Scrutiny reservation by NL, related to Article 1(4).

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

(…)[39]

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 existing at the time of adoption of the Framework Decision.
In the application of these agreements, the transfer to a third State of personal data obtained from another Member State, shall be carried out while respecting the provisions of Article 14(1)(c) and (2) on prior consent.

Article 27a

Evaluation

1. Three years after expiry of the period laid down in Article 28(1), Member States shall report to the Commission on the national measures they have taken to ensure full compliance with this Framework Decision, and particularly also with regard to those provisions that already have to be complied with when data is collected. The Commission shall examine in particular the implications of the provision on scope in Article 1(2) .

[39] See draft Council declaration set out in Annex II.

2. The Commission shall report to the Council and the European Parliament within one year on the outcome of the evaluation referred to in paragraph 1, and shall accompany its report with any appropriate proposals for amendments.

Article 27b

Relationship to other Council acts

In cases where (…) in an act adopted under Title VI of the Treaty on European Union specific provisions for the protection of personal data are laid down, these provisions are laid down (…), these conditions shall take precedence over the provisions of this Framework Decision governing the same aspects. Matters not regulated by the Council act shall be governed by the relevant provision of this Framework Decision[40].

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 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 … assess the extent to which Member States have taken the measures necessary to comply with this Framework Decision.

[40] BE, CH, GR and HU scrutiny reservation.

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

DRAFT COUNCIL DECLARATION

""In the future, in accordance with the applicable legal bases, functions performed by the existing common data protection supervisory authorities, which have (...) been established separately for the Schengen Information System, Europol, Eurojust, and the (...) Customs Information System, should be combined within a single data protection supervisory authority, whilst taking account of the specific nature of these systems and bodies."[41]

[41] Eurojust, supported by AT and NL, demanded that Eurojust be omitted from this Declaration.