COUNCIL OF THE EUROPEAN UNION

Brussels, 13 July 2007

Interinstitutional File: 2005/0202 (CNS)

11365/07

LIMITE

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

NOTE

from :	Presidency
to :	Multidisciplinary group on organised crime
Nos prev. doc :	7315/2/07 REV 2 CRIMORG 53 DROIPEN 18 ENFOPOL 45 DATAPROTECT 10 COMIX 267 ENFOCUSTOM 30
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 21 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

The Conference of European Data Protection Authorities has delivered two opinions [2] on the proposal. The Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Data also has given some initial remarks on the draft Framework Decision[3].

2. The Commission presented its proposal to the meeting of the Multidisciplinary group on organised crime (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.

3. The German Presidency submitted a thoroughly revised draft [4] to the Article 36 Committee at its meeting on 23 March 2007. The MDG-Mixed Committee finalised a second reading of this revised draft on 6 June 2007 and commenced a third reading at its meeting of 15 June 2007. The attached text, which was established with the help of the outgoing Presidency, which the current Presidency gratefully acknowledges, seeks to render the situation as per the end of the second reading. It therefore takes account of the discussions which were held on 6 June, but not of those on 15 June 2007. Only the changes compared to 7315/2/07 REV 2 CRIMORG 53 DROIPEN 18 ENFOPOL 45 DATAPROTECT 10 COMIX 267 ENFOCUSTOM 30 have been underlined. The latter document already contained the results of the second reading regarding Article 1-16.

4. Delegations are invited to continue the third reading as from Article 17 onwards at the MDG-COMIX meeting of 18 July 2007. After the finalisation of third reading, the Presidency will establish a new revised draft of the Framework Decision.

5. SE, DK and IE have entered a parliamentary scrutiny reservation.

---

2 6329/06 CRIMORG 28 DROIPEN 12 ENFOPOL 26 DATAPROTECT 4 COMIX 156; 9821/07 CRIMORG 88 DROIPEN 44 ENFOPOL 98 DATAPROTECT 21 COMIX 480 ENFOCUSTOM 55.

3 8274/07 CRIMORG 68 DROIPEN 32 ENFOPOL 61 DATAPROTECT 14 COMIX 349 ENFOCUSTOM 40.

4 7315/07 CRIMORG 53 DROIPEN 18 ENFOPOL 45 DATAPROTECT 10 COMIX 267.

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,[5]

Having regard to the opinion of the European Parliament,[6]

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.

---

5 …

6 …

(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* [7].

(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 [8] 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.

---

[7] OJ C 198, 12.8.2005, p. 1.

[8] 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) Data are also erased if the data medium is destroyed.

(6) (…)

(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.[9]

(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) The principle of data accuracy 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 principle 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.]

[9] Many delegations had asked that this recital be recast.

(8b) Archiving in a separate data set is permissible only if the data are no longer required and used for purposes laid down in Title VI of the Treaty on European Union. 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 purposes laid down in Title VI of the Treaty on European Union. 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.

(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 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.

(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 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 [10] 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) [11].

(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 [12] (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.

---

[10] OJ L 8, 12.1.2001, p. 1.
[11] OJ L 201, 31.7.2001, p. 37.
[12] OJ L 239, 22.9.2000, p. 19.

(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.

(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 [13].

(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 or the Additional Protocol to that Convention of 8 November 2001.

[13] 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 [14].

(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.

[14] OJ L 131, 1.6.2000, p. 43.

(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 [15].

(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 [16].

(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.

(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,

---

[15] OJ L 176, 10.7.1999, p. 31.
[16] 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 Member State or from authorities or information systems established on the basis of Council acts. [17]

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 specific intelligence activities in the field of national security.[18]

[17] Scrutiny reservations by AT, IT, FR, CZ, IE, FI, LU and CY. Reservations by BE and ES.

[18] Scrutiny reservations by AT, PL, IE, UK, NL and ES. The restriction proposed specifically to intelligence activities received the express backing of SE, HU, BE, AT, UK, PL, FR, ES, IT, GR, NO, DK and COM.

5. This Framework Decision shall not preclude Member States from providing safeguards for the protection of personal data higher than those established in this Framework Decision. (...) Member States shall, however, ensure that data transmissions to other Member States or to authorities established pursuant to Title VI of the Treaty on European Union shall not be subjected to higher safeguards than similar national data transmissions.[19]

Article 2

Definitions[20]

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;[21]

(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;

---

19 Scrutiny reservation by DK.
20 Scrutiny reservation by IT.
21 Reservations by FR and SI.

(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;[22]

(h) [23];

(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[24];

(j) "controller" shall mean the 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[25];

---

22 Reservations on consent by COM, IT and GR.

23 Since this concept occurs only once in the Framework Decision (Article 14), the definition has been transferred to the article concerned. At the same time, the Commission's point that data should be passed to an international body solely for specific purposes and that the recipient international body or organisation must be one which is responsible for the prevention, investigation, detection or prosecution of criminal offences has been taken into account.

24 The addition regarding responsibility was deleted since the definition of controller has been reinstated.

25 Following the request by a number of delegations (AT, FR, GR, HU, PT and SK) in favour of retaining the definition of controller, the text is aligned on the definition in Article 2, point (d) of Directive 95/46/EC.

(k) "marking"[26] shall mean the marking of stored personal data without the aim of limiting their processing in future;[27]

(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[28] be attributed to an identified or identifiable individual.

Article 3

Principles of lawfulness, proportionality and purpose[29]

1. Personal data may 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.[30] Processing of the data must be legitimate and adequate, relevant and not excessive.[31]

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;

   (b) the competent authorities are authorised to process such data [32] in accordance with the legal provisions applicable and;

---

26 "marking" replaced by "referencing". SE rightly pointed out that the English translation did not correspond to the Prüm Convention.

27 Reservations by DK and SE. The Prüm Convention also contains rules on referencing, which implies that Member States will have to allow for corresponding possibilities under national law in that connection. Article 18(2) provides merely for the possibility of referencing instead of compulsory referencing.

28 GR entered a reservation and asked (like AT) that the alternative "or only with disproportionate investment of time, cost and labour" be deleted. This definition, which does not appear in Directive 95/46, consitutes a clear improvement in terms of data protection. An alternative is to delete the definition, leaving Member States completely free to interpret the concept as they wish.

29 Scrutiny reservations by FR, ES, CH, DK, CZ, IE and GR.

30 Aligned on Article 6(1)(b) of Directive 95/46.

31 Aligned on Article 6(1)(c) of Directive 95/46.

32 Scrutiny reservation by COM. Wording intended to meet the concerns of AT and COM.

(c) processing is necessary [33] and appropriate to that purpose.

Article 4

Correction requirement

Personal data shall be corrected if inaccurate and, where this is possible and necessary,[34] completed or updated.

Article 5

Erasure[35] 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 further processed. Archiving of data in a separate database for an appropriate period in accordance with national law shall not be affected by this provision.[36]

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 which prevented their erasure.

---

33 At the request of DK, ES, NL and FR "essential" was changed to "necessary".

34 UK proposal, which also takes into account the concerns expressed by BE.

35 "Destruction" is no longer referred to separately. In Directive 95/46/EC, too, it appears only in the definition of data processing. The new recital 5b makes clear that "erasure" is to be assumed if the data medium is "destroyed".

36 Reservation by GR. Scrutiny reservation by PT. The rule on archiving was supported by numerous delegations (CH, ES, UK, BE, PT, DK, RO, SL, AT, LU, FI and IT and should therefore be retained. Account was taken of the concerns voiced by ES and UK by adding a new recital 8b.

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.[37]

Article 8

Automated individual decisions[38]

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.

---

[37] The previous wording was too restrictive for some delegations (CZ and DK) while for other delegations it was already too broad (AT, ES, BE, HU, PT and COM). The current wording is closer to Article 6 of Council of Europe Convention No 108.

[38] Scrutiny reservation by DK.

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[39] 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[40] 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[41] transmitted, the recipient must be notified without delay. The data must be corrected, erased, or blocked without delay unless such data are the content of a court ruling.[42]

---

39 Proposed by AT.

40 Proposed by AT.

41 The text is intended to clarify and takes account of SE's objection.

42 Reservation by BE. The text takes into account the wishes of SE, UK and CH that there is no obligation to erase if unlawfully transmitted data has led to a criminal conviction. The provision does not hinder the resumption of judicial proceedings.

Article 10

Compliance with time-limits for erasure and review[43]

The transmitting authority[44] shall, upon transmission or making available of the data, indicate the time-limits in accordance with Article 5[45] for the retention of data provided for under its national law, following the expiry of which the recipient must also erase or block the data or review whether or not they are still needed. Erasure or blocking may be waived if the data are required for a current investigation, prosecution of crimes or enforcement of criminal penalties and if in such a case erasure or blocking must also be waived under the national law of the transmitting authority.[46]

Article 11

Logging and documentation[47]

1. All transmissions[48] 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.

---

43 Scrutiny reservations by SE, DK and UK.

44 "authority" instead of "body" (see Article 2(i)).

45 The reference to Article 5 takes up a proposal by CH, SE, SK and RO and makes it clear that it is also possible to archive the data transmitted.

46 UK asked whether the provision in the second and third sentences were not too restrictive in contrast with Articles 5 and 6. It was pointed out that the 2nd and 3rd sentences referred only to time limits for erasure while Articles 5 and 6 also provided for the possibilities of time limits for review. The assumption is that time limits for review were the norm in Member States and that strict time limits for erasure without the possibility of further use on expiry of the time limit were rather the exception. If the national law provides for time limits for erasure within the meaning of Article 5(1), according to which data are to be erased if it is no longer necessary to store them, and if only the requirement for strict time limits is reviewed, the transmitting authority will merely point this out. If, however, the national law of the transmitting authority provides exceptionally for absolute time limits for erasure, these must also apply to the data transmitted since the time limits could otherwise be circumvented.

47 Scrutiny reservation by CZ.

48 CZ proposed that, here too, data made available be dealt with separately. It is doubtful whether this is necessary, since automatic data retrieval comes under the general concept of "transmission".

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.

Article 12

Purpose of personal data received from or made available by another Member State[49]

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[50]; or

   (d) any other purpose only with the prior consent of the transmitting Member State or with the consent[51] 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.

---

49 Scrutiny reservations by CH, IT, BE, LU, DK, ES, HU, FR, PL and AT.

50 Scrutiny reservation by NL.

51 The vast majority of Member States wishes to retain the possibility of consent of the data subject. These possibilities are contained in particular also in Article 23(1)(d) of the European mutual legal assistance agreement and in Article 10(1) of the Framework Decision on the European arrest warrant.

2. In cases where appropriate specific[52] 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.[53]

Article 13

Compliance with particular national processing restrictions[54]

The transmitting authority shall inform the recipient of particular[55] 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[56]

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,

---

52 The addition is designed to meet the concerns of FR.
53 Scrutiny reservations by PL and NL.
54 Scrutiny reservation by NL.
55 Proposal by SE , which also may accommodate the concerns of other delegations (CZ, UK and ES). The insertion of the word "particular" makes it clear that this does not concern the general processing restrictions which already apply on the basis of this Framework Decision.
56 Reservation by SE. Scrutiny reservations by CZ, FI, HU and IT. It is pointed out that the Member States may also adopt higher safeguards (Article 1(5)) and that compliance with those higher safeguards is already ensured by the requirement for consent.

(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

(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 and the prior consent cannot be obtained in good time.[57]

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 appropriate safeguards which are deemed adequate by the Member State concerned according to its national law.[58]

[57] Proposal by UK here, which provides for an exception to the requirement for consent in urgent cases. This provision would appear to be advisable on technical grounds, since it cannot always be assumed that consent can be obtained at short notice.

[58] Scrutiny reservation by AT.

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.[59]

Article 14a

Transmission to private parties[60]

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 person prevent transmission and
   (c) in particular cases transfer is essential for the competent authority[61] 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.

---

[59] The proposal is aligned on Article 25(2) of Directive 95/46/3C.

[60] Scrutiny reservations by AT, BE, GR, PT, SE, PL, IT, DK and SK. This provision does not involve the transfer of police or judicial tasks to private parties. The communication of personal data by the judiciary or police is, however, necessary in many cases to prosecute crime or avert threats. For example, the police may have to issue alerts concerning forgeries of securities to banks and credit institutions. In the area of vehicle crime, the police need to communicate information 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.

[61] LU proposal.

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.

Article 16

Information for the data subject[62]

The Member States shall ensure that the competent authority informs the data subject of the fact that personal data are being collected, of the categories of data involved, of the controller[63] 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 the particular case, to be incompatible with the permissible purposes[64] of the processing;

2. involves a disproportionate effort compared to the legitimate interests of the data subject;

3. the information is already available to the data subject, or

4. the collection or further processing of personal data - in particular further processing for statistical purposes or for the purposes of historical or scientific research - is expressly provided for by law. [65]

---

[62] Reservation by IE. Scrutiny reservations by FI, CZ, NL, DK, GR, IT, RO, NO, PL and SK.

[63] Proposal by AT and GR.

[64] Permissible purposes include all the purposes referred to in Article 12(1). It does not consider it necessary, therefore, to make separate or explicit reference here to the purposes of the prevention, investigation, detection or prosecution of criminal offences, in particular.

[65] Proposal by AT, which is aligned on the further exception contained in Article 11(2) of Directive 95/46/EC. At the same time it takes into account the concerns of those delegations that were in favour of a more flexible provision (IE, DK, SK, BE, IT and FR).

Article 17

Right of access [66]

1. Every data subject is entitled, on request, to receive from the competent authority, directly or through the intermediary of the national supervisory authority, without constraint and at appropriate intervals [67] 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; or

   (c) confirmation that all necessary verifications have taken place[68].

2. The Member States may adopt legislative measures [69] restricting access to information pursuant to paragraph 1, where such a restriction, with due regard for the legitimate interests of the person concerned, constitutes a necessary and proportional measure: [70]

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

   (b) for the prevention, investigation, detection or prosecution of criminal offences; [71]

   (c) for protecting public security;

   (d) for protecting national security; [72]

---

66 FI, IT, DK, BE, CZ, GR and IE scrutiny reservations.
67 Proposal by SE which reflects Article 12(a) of Directive 95/46/EC.
68 Suggestion by BE and FR.
69 Some delegations (BE, DK) asked that a reference to national law be inserted. Therefore a wording which is closer to Article 13(1) of Directive 95/46/EC, has been put forward.
70 Scrutiny reservation by IE.
71 Reflects Article 13(1)(d) of Directive 95/46/EC.
72 Reflects Article 13(1)(a) of Directive 95/46/EC.

(e) for protection of the data subject or of the rights and freedoms of others [73].

3. [74]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. Member States may also provide that notification by a national supervisory authority may be limited to informing the data subject that a review has taken place. [75] In all of these cases the data subject shall be advised that he may appeal to the competent national supervisory authority [76]. 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 [77]. (…)

---

73 Proposal by AT, reflects Article 13(1)(g) of Directive 95/46/EC.

74 Scrutiny reservation by BE concerning paragraph 3.

75 Proposal by FR.

76 The additions were deleted after numerous delegations expressed concerns and because the additions in question were not absolutely necessary. Where the courts are competent under national law, the following sentence applies.

77 Deleted at the request of FR and GR.

Article 18

Right to rectification, erasure or blocking [78]

1. The data subject is entitled to expect the controller to fulfil its duties in accordance with Articles 4 and 5 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 [79] 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. [80]

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. [81]

---

[78] Some delegations advocated joining Articles 17 and 18 together again (FR, NL, BU and LU). FI welcomed the separation and wanted it to remain. The Presidency proposed supplementing Article 18 to take account of the concerns of FR, NL, BU and LU and the differences between granting access on the one hand and rectification, erasure, destruction or blocking on the other hand. As the duties in accordance with Articles 4 and 5 concerning rectification, erasure, destruction or blocking apply without exception, Article 18 does not extend these duties but merely guarantees the subjective right to expect compliance by the authorities with their objective duties in accordance with Articles 4 and 5.

[79] The question of which authority the complaint or application for judicial remedy should be made to does not need to be regulated at EU level.

[80] Proposed by FR and BE.

[81] DK scrutiny reservation. It is emphasised that paragraph 2 is an optional provision. The current proposal incorporates the concerns expressed by some delegations (IE, NL, FR and PT), without renouncing the use of referencing.

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 competent authority or other authority competent under national law 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 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 [82] 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.

[82] Proposed by NL.

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 [83]:

   (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);

[83] CZ scrutiny reservation.

(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 checking [84]

Member States shall ensure that the competent national supervisory authorities are consulted prior to the processing of an indefinite quantity[85] of personal data which will form part of a new filing system to be created or a new procedure 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.

Article 25

National supervisory authorities [86]

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.

---

[84] The term was changed (from "prior consultation") at the suggestion of AT. Scrutiny reservations by AT, NL and BE.

[85] ES scrutiny reservation.

[86] Scrutiny reservation by NL.

2. Each authority shall be endowed in particular with: [87]

(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.

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.

5. Courts shall be subject to supervision by national supervisory authorities only in so far as they take action in administrative matters. [88] *[alternative: The supervisory authority's powers do not extend to the justice authorities when acting in their judicial capacity.]*

---

87 Scrutiny reservation by CZ.

88 The provision should take account of the requirements of the separation of powers and/or the independence of the judiciary. Member States are nevertheless free to lay down (special) supervisory mechanisms for courts in national law.

Article 26

Joint supervisory authority [89]

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.

[89] Eurojust is opposed to his proposal. COM, AT, IT, NL and SE also were of the opinion that that the structure of a joint supervisory authority should take account of Eurojust's special characteristics. DK scrutiny reservation.

Article 27

Relationship to Agreements with third States[90]

This Framework Decision is without prejudice to any obligations and commitments incumbent upon Member States or upon the European Union by virtue of existing[91] bilateral and/or multilateral agreements with third States. [92]

Article 27a

Evaluation

1. Four 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 also examine whether the provisions on scope in Article 1(2) in practice lead to data not being transmitted to other Member States or authorities or information systems of the European Union because the provisions of the Framework Decision have not been applied comprehensively at national level.

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.

---

90 Scrutiny reservation by FR and GR, which pleaded in favour of the deletion of this provision and think only Article 14 should apply to this matter. However, this would imply a need to repeal or renegotiate existing agreements whose data protection arrangements are not in full compliance with the DPFD. This does not seem realistic and therefore the DPFD requirements should apply solely to future agreement with third countries, as is also set out in recital 24. It is recalled that Article 14 can nevertheless apply where a Member State's existing agreement with third countries does not provide for any obligation to exchange data, or where the existing agreement also stipulates that data exchange is to take place in accordance with current national law.

91 UK argued in favour of the deletion of the word 'existing'.

92 With regard to the relationship with Council of Europe Convention No 108 of 28 January 1981, see recital 25.

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 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