COUNCIL OF THE EUROPEAN UNION

Brussels, 9 October 2006

Interinstitutional File: 2005/0202 (CNS)

13246/1/06 REV 1

LIMITE

CRIMORG 143
DROIPEN 61
ENFOPOL 161
DATAPROTECT 33
COMIX 780

NOTE

From :	Presidency
To :	Multidisciplinary Group on Organised Crime
No. prev. doc. :	13426/06 CRIMORG 143 DROIPEN 61 ENFOPOL 161 DATAPROTECT 33 COMIX 780
Subject :	Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

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 co-operation in criminal matters ('DPFD') to the Secretary-General of the Council. On 13 December 2005, the Council asked the Parliament for its opinion on the proposal. The Parliament delivered its opinion on 27 September 2006. The European Data Protection Supervisor has also delivered his opinion on the proposal[1], which he presented to the MDG-Mixed Committee on 12 January 2006. On 24 January 2006, the Conference of European Data Protection Authorities also delivered an opinion on the proposal[2].

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

On 11 January 2006, the Hungarian delegation submitted an extensive note on the Commission proposal[3].

DE, DK, LV, NL, PT, SE and SI have a general scrutiny reservation on the proposal. DK, FR, IE, HU, NL, SE, SI and UK have a parliamentary reservation. AT, ES, FR, FI, IT and SE have a linguistic scrutiny reservation.

2. The Commission presented its proposal to the Multidisciplinary group on organised crime (MDG) - Mixed Committee on 9 November 2005. At the MDG meeting on 21-22 September 2006, the first reading of the DPFD was finalised. At the MDG meeting of 3-4 October 2006 delegations commenced the second reading, up to Article 26.

3. Regarding the MDG meeting on 19 October 2006, the Presidency invites delegations to continue the second reading as from Article 27 onwards and, after that, to commence the third reading. Regarding the third reading, a few of the main open issues have been further clarified hereafter. The Presidency would like to emphasise that is list is by no means exhaustive and that it will try to discuss as many items as possible at the MDG meeting on 19 October 2006.

4. **Article 1**

The Presidency intends to bring the general question of the scope (only internationally exchanged data or also domestic data) to the Article 36 Committee on 23-24 October 2006 (and Coreper). Whilst the Presidency acknowledges that this important question still needs to be decided, the current draft departs from the point of view that the Framework Decision will also be applicable to domestic data processing.

[3] 5193/06 CRIMORG 3 DROIPEN 2 ENFOPOL 3 DATAPROTECT 1 COMIX 26.

5. **Article 5**

The Presidency has redrafted Article 5, in particular paragraph 3. At the MDG meeting on 3 and 4 October, it was clear that a majority of delegations wanted the Framework Decision to distinguish clearly between the purposes for which personal data may be processed in a domestic context and the purposes for which data that have been received from another Member State may be processed. In this regard the Presidency would like to emphasise the following:

1) Article 5(3) applies solely to domestic data processing (as is made clear by Article 11(1)); and
2) Article 5(3) is an optional provision with minimum standards. This means that Member States are not obliged to allow data processing for each of the purposes set out in Article 5(3), but that they may adopt stricter rules.

The Presidency hopes that this clarification will make it easier for delegations to agree on the proposed wording for Article 5(3). Some delegations, have, questioned the need or indeed the possibility to define the purposes for which law enforcement data may be processed at domestic level in precise terms in the Framework Decision. Whilst the Presidency is willing to discuss any alternative proposal, it would like to point out that this might imply a return to the original Commission wording ("or lawful purposes not incompatible with the original purposes"), which was opposed by a significant number delegations (BE, CH, ES, GR, PT and SE) at an earlier meeting.

Can delegations accept that the current text?

6. **Article 11(1)**

The new drafting of Article 11 makes it clear that this provision applies solely to cross-border data processing. It sets out the purposes for which personal data may be used other than the ones for which they were transmitted. Apart from Article 11(1)(iv), these purposes are similar to those set out in Article 23 of the 2000 Mutual Assistance Convention.

In order to deal with all operational law enforcement concerns, the Presidency had proposed a new text for Article 11(2), which allows Member States to require a prior consent for further processing in exceptional cases. The Presidency acknowledges that concept of exceptionally sensitive cases may need to be reworded and invites delegations to make text proposals to that effect.

The Presidency has also made a proposal for a new paragraph 2a, which is inspired by Article 23(2) of the 2000 Mutual Assistance Convention. The Presidency thought delegations might want to retain the possibility which exists under that Convention (but maybe under other co-operation instruments as well) to place conditions on the use of very specific types of information (e.g. transcripts of telephone wiring, results of JITs, etc.).

Can delegations agree to the new text of Article 11?

7. **Article 15**

Further to the comments made at the meeting on 3 and 4 October 2006, the Presidency has further revised the text of this provision. The Presidency is of the opinion that the proposed DPFD regime for the exchange of data with third countries should apply to all, including purely domestic, data. Should, however, the decision be taken to exclude domestic data processing from the scope of the DPFD, all references in Article 15 to an adequacy requirement should be deleted and Article 15 should be confined to the text currently in Article 15(1)(a)(b) and (c).

Can delegations accept the current text, it being understood that it might have to be changed in case the decision were to be taken to exclude domestic data processing from the scope of the DPFD.

8. Delegations are invited to finalise the second reading and commence the third reading of the draft Framework Decision.

ANNEX

COUNCIL FRAMEWORK DECISION

of ....

on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 30, Article 31 and Article 34 (2)(b) thereof,

Having regard to the proposal from the Commission,[4]

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

Whereas:

(1) The European Union has set itself the objective to maintain and develop the Union as an area of freedom, security and justice; a high level of safety shall be provided by common action among the Member States in the fields of police and judicial cooperation in criminal matters.

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

---

4 …

5 …

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

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

(5) The exchange of personal data in the framework of police and judicial cooperation in criminal matters, notably under the principle of availability of information as laid down in the Hague Programme, should be supported by clear binding rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way excluding any obstruction of this cooperation between the Member States while fully respecting fundamental rights of individuals. Existing instruments at the European level do not suffice. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[7] does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security and the activities of the State in areas of criminal law.

---

6 OJ C 198, 12.8.2005, p. 1.

7 OJ L 281, 23.11.1995, p. 31.

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

(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 jeopardized in any way.

(8a) The principle of accuracy of data has to be applied in the light of the nature and the purpose of the specific processing. Especially in the course of judicial proceedings data are based on the perception of a person and in some cases those data cannot be verified at all. Thus, the principle of accuracy cannot refer to the accuracy of a statement but merely to the fact that a person has given a specific statement. Also, it has to be considered that in some cases files – and, therefore, data – will be partially verified as to their content but that those data might remain in the files, for example for documentation purposes[8].

[8] This recital is meant to explain the concept of accuracy of Article 4(1)(d). Scrutiny reservation by SE and SI. ES thought the wording should be adapted so as to bring police work more clearly in its scope.

(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) This Framework Decision should define the procedure for the adoption of the measures necessary in order to assess the level of data protection in a third country or international body.

(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. Furthermore, it is necessary that Member States provide for criminal sanctions for particularly serious and intentionally committed infringements of data protection provisions.

(15a) Whereas 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[9].

[9] To be read in conjunction with Article 23.

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

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

(18) A Working Party on the protection of individuals with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences should be set up and be completely independent in the performance of its functions. It should advise the Commission and the Member States and, in particular, contribute to a uniform application of the national rules adopted pursuant to this Framework Decision.

(19) Article 47 of the Treaty on European Union provides 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].

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

(20) The present Framework Decision is without prejudice to the specific data protection provisions laid down in the relevant legal instruments relating to the processing and protection of personal data by Europol, Eurojust and the Customs Information System.

(21) The provisions regarding the protection of personal data, provided for under 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 rules of this Framework Decision for the purposes of matters falling within the scope of the EU Treaty.

(22) It is appropriate that this Framework Decision 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 as foreseen in the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems[13].

(24) It is appropriate to replace Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[14].

(25) Any reference to the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal data should be read as reference to this Framework Decision.

---

12 OJ L 239, 22.9.2000, p. 19.
13 OJ L 69, 16.3.2005, p. 67.
14 OJ C 197, 12.7.2000, p. 3.

(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 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 [15].

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

(29) As regards Iceland and Norway, this Framework Decision constitutes a development of provisions of the Schengen acquis within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis, which fall within the area referred to in Article 1(H) of Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of that Agreement[16].

---

15 OJ L 131, 1.6.2000, p. 43.

16 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) 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[17].

(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 recognized, 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,

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

HAS ADOPTED THIS FRAMEWORK DECISION:

CHAPTER I
OBJECT, DEFINITIONS AND SCOPE

Article 1

Object and scope

1. This Framework Decision determines common standards to ensure the protection of individuals with regard to the processing of personal data in the framework of police and judicial co-operation in criminal matters, provided for by Title VI of the Treaty on European Union[18], while safeguarding citizens' freedom and providing them with a high level of safety.

2. 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 by a competent authority for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[19].

---

[18] CH, CZ, DK, IE and UK thought the scope of the draft Framework Decision should be confined to transfer of data between Member States and should not cover data which are processed in a purely domestic context. SE thought the scope of the draft Framework decision should be transfer of data between Member States, but that it would also have an impact on the domestic handling of data on a general level. COM, BE, FR, and PT thought it should also apply to domestic data processing.

[19] Scrutiny reservation by CH, DK and SE.

3. This Framework Decision shall not apply to the data protection regimes established by or by virtue of

– the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention)[20],

– the Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime[21],

– the Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, and any amendments made thereto[22].

(...) This Framework Decision is without prejudice to essential national security interests.

4. This Framework Decision does not preclude Member States to provide safeguards for the protection of personal data in the context of police and judicial cooperation in criminal matters higher than those established in this Framework Decision, but such provisions may not restrict nor prohibit the disclosure of personal data to the competent authorities of other Member States for reasons connected with the protection of personal data as provided for in this Framework Decision[23].

---

[20] OJ C 316, 27.11.1995, p. 2. Convention as last amended by the Protocol drawn up on the basis of Article 43(1) of the Europol Convention (OJ C 2, 6.1.2004, p. 3).

[21] OJ L 63, 6.3.2002, p. 1. Decision as last amended by Decision 2003/659/JHA (OJ L 245, 29.9.2003, p. 44).

[22] New language proposed by the Presidency so as to accommodate previously expressed concerns HU, IT and SE. DK and ES thought the Schengen Information System should also be excluded from the scope of the draft Framework Decision.

[23] Scrutiny reservation by AT, BE, COM, DE, GR, IT and NL.

Article 2

Definitions

For the purposes of this Framework Decision:

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

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

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

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

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

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

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not;

(h) '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;

(i) 'international bodies' shall mean bodies or organisations established by international agreements[24];

(j) 'competent authorities' shall mean police, customs, judicial and other competent authorities of the Member States that are authorized by national law to detect, prevent, investigate or prosecute offences or criminal activities or to execute criminal penalties within the meaning of Article 29 of the Treaty on European Union or to handle data for the furtherance of one of these goals[25].

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

(l) blocking' shall mean the marking of stored personal data with the aim of limiting their processing in future

[24] Reservation from DK.

[25] CZ and SI reservation: these delegations wanted to redraft the text so as to encompass the Ministry of Justice. The Presidency hopes the proposed text can accommodate these concerns.

[26] Reservation by NL and SE. NL is opposed to the introduction of the concept of marking in the DPFD. SE thinks there is no need of a definition of marking. So did the UK delegation, but it could accept the definition.

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

Article 4

Principles relating to data quality

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

   (a) processed fairly and lawfully;

   (b) collected for specified, explicit and legitimate purposes[27];

   (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed[28];

   (d) accurate[29] and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected, for which they are further processed are erased or rectified. Member States may provide for the processing of data to varying degrees of accuracy and reliability in which case they may provide that data are distinguished, as far as practicable, in accordance with their degree of accuracy and reliability[30];

   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

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

---

27 DK, UK and COM asked that the following language from the Data Protection Directive be added: ' and not further processed in a way incompatible with those purposes '. The Presidency agrees with BE and DE that this is regulated in Article 5.

28 Language from the Data Protection Directive inserted at the request of BE, COM, DE, DK, ES, FR, NL, MT, PT and UK.

29 Scrutiny reservation by DE, SE and SI..

30 IE reserve on second sentence.

Article 5

Criteria for making data processing legitimate[31]

1. Member States shall provide that personal data may be processed by the competent authorities only if provided for by law.

2. Member States shall provide that processing of personal data is only legitimate as far as it is necessary[32] for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[33].

3. Member States may provide that the further processing[34] of data is legitimate if the data subject concerned has given its consent[35] therefore, or if it is necessary for the following purposes:

i) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which the original processing took place; or

ii) for other judicial, administrative and regulatory[36] purposes directly related to purposes referred to in paragraph 2; or

iii) the protection of the rights and freedoms of a person; or

---

31 AT, DE, IE, IT, MT and PT scrutiny reservation.

32 This text was inspired by the text of article 8(2) ECHR. However, DE and SE would prefer to use the term "proportional" instead of "necessary".

33 UK scrutiny reservation on the reference to the execution of the penalties: the UK thinks this already implicitly implied and does not explicit mentioning.

34 DE would prefer to specify the concept of 'further processing' as 'processing for purposes other than those for which the original processing took place'.

35 COM, ES, GR and HU were opposed to the use of consent in a law enforcement context. Other delegations were, however, insistent that this be acknowledged as valid legal basis for further processing.

36 BE and Pl questioned the use of the concept 'regulatory'.

iv) the prevention of threats to public security; or

v) for other lawful purposes of substantial public interest not incompatible with the purposes referred to in paragraph 2 ; or

vi) historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as, for example, anonymising the names of the persons concerned.

Article 6

Processing of special categories of data[37]

In addition to the conditions laid down in Article 5, Member States shall permit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life only when this is strictly necessary. Member State shall provide for suitable additional safeguards.

[37] Scrutiny reservations by DE and DK. Some delegations wanted to return to the original Commission proposal (AT, SI), but there was clearly no support for that. BE asked that a rule similar to that used in the Europol context inserted here. No delegation expressed supported for this proposal.

Article 7

Time limits for storage of personal data [38]

1. Member States shall provide that automated personal data shall be stored only as long as it is necessary for the purpose for which it was collected or further processed. Non-automated personal data shall be archived or destroyed when it is no longer necessary to store them for the purpose for which it was collected or further processed[39]

2. Member States shall provide for appropriate time limits for the storage of personal data or for a periodic review of the necessity of the storage and shall provide for procedural (...) measures to ensure that these are observed. Personal data shall be deleted if a review shows that their storage is no longer necessary[40].

[38] Scrutiny reservation by NL.

[39] Text proposal in order to accommodate the concerns of various delegations (ES, PT, MT, HU, DK, BE), who thought that the text should be changed so as to take specific account of paper files, notably in judicial files.

[40] FR scrutiny reservation.

CHAPTER III – Specific Forms of Processing

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

Article 8

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

(...)[41]

Article 9

Verification of quality of data that are transmitted or made available[42]

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

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

[41] DE, DK, ES, PL, SE and UK thought Article 8 was redundant. AT, COM, GR and NL thought it should be retained. As Chapter II, as the Presidency reads it, applies also to the cross-border transmission of information of data (with the exception of Article 5(3)), Article 8 did indeed seem to restate the obvious. The Presidency has therefore deleted it.

[42] DK and SE thought that this provision was still too detailed.

3. Member States shall provide that a competent authority that transmitted or made available personal data to a competent authority of another Member State shall inform the latter immediately if it should emerge, from a notification by the data subject or otherwise, that the data concerned should not have been transmitted or made available or that inaccurate or outdated data were transmitted or made available[43]. If the receiving authority has reasonable grounds to believe that received personal data are inaccurate or to be deleted, it shall inform without delay the competent authority that transmitted or made available the data concerned.

4. (...)[44]

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

– if these data should not have been transmitted, made available or received[45],

– after a time limit laid down in the law of the other Member State if the authority that transmitted or made available the data concerned has informed the receiving authority of such a time limit when the data concerned were transmitted or made available, unless the personal data are further needed for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[46],

– [47].

---

43 The Presidency agrees that care should be taken that this paragraph could not be applied retroactively, i.e. to data exchanged before the entry into force of this Framework Decision. This will need to be examined in the context of the final provisions of the Framework Decision.

44 The content of this paragraph has been moved to Article 21(1)(bb) at the request of several delegations.

45 Reinstatement of original text at the request of DE and NL.

46 CZ, DE and DK scrutiny reservation. There may be absolute time limits under domestic law. The question as to whether the internal time limits of the transmitting Member State should be binding on the receiving Member State, will need to be further discussed.

47 This text (' if these data are not or no longer necessary for the purpose for which they were transmitted or made available') was deleted because this rule already exists by virtue of Article 7(1). DE scrutiny reservation.

6 Personal data shall not be deleted but blocked in accordance with national law if there are reasonable grounds to believe that the deletion could affect the interests of the data subject worthy of protection. Blocked data shall only be used or transmitted for the purpose they were not deleted for[48].

Article 10

Logging and documentation[49]

1. Member States shall aim to ensure that[50] all exchanges of personal data are logged or documented [for the purposes of verification of the admissibility of data searches and the lawfulness of the data processing, self-monitoring, ensuring proper data integrity and security][51].

2. The authority that has logged or documented such information shall communicate it without delay to the competent supervisory authority on request of the latter. The 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 (...)[52].

---

48 ES thought the legal consequences of blocking should be better defined.

49 AT would have preferred that the provision list the data to be logged, as is the case in Article 39 of the Prüm Treaty. AT, BE and HU would have preferred the rules on logging to be generally applicable rules, also for domestic situations.

50 CZ and GR asked that the words "every access to" be reinstated.

51 IE proposed that the language between square brackets be deleted.

52 Deleted at the request of several delegations (DK, IE and IT). COM, HU and SI opposed the deletion.

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

Article 11

Further processing (...) of personal data received from or made available by the competent authority of another Member State

1. By way of derogation from Article 5(3), Member States shall provide that personal data received from or made available by the competent authority of another Member State may be further processed or made available to other authorities of another Member State only for one of the following purposes:

   i) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which the original processing took place; or

   ii) for other judicial, administrative and regulatory[53] purposes directly related to purposes referred to in Article 5(2); or

   iii) the prevention of serious and immediate threats to public security; or

   iv) historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as, for example, anonymising the names of the persons concerned;

   v) for any other purpose, only with the prior consent of the competent authority that has transmitted or made available the personal data

[53] BE and PL questioned the use of the concept 'regulatory'.

2. In cases (...) of an exceptionally sensitive nature[54], the competent authority that transmitted or made available the personal data may require that its prior consent be obtained for the processing of these data for any purpose other the ones for which these data were transmitted.

2a. Where the legal instrument on the basis of which the personal data are transmitted or made available allows to impose certain conditions on the use of specific types of information, these conditions shall prevail. If no conditions are imposed, this article shall apply[55].

3. (...)[56]

[54] BE, CH, FR, GR and HU asked what the exact content of this concept was.

[55] Presidency proposal inspired by Article 23(2) of the 2000 Mutual Assistance Convention.

[56] Various delegations (BE, DE, DK, NL, SE and UK) agreed to delete this paragraph. This question of the relationship of this Framework Decision to other, more specific data protection provisions, has to be dealt with in a general way. The Presidency is of the opinion that this proposal only makes sense if delegations agree that this Framework Decision will supersede the data protection regime (including the specialty principle) provided for in Article 39 Schengen Implementation Convention and, in the future, the Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union. However, the Presidency also agrees that it needs to be examined whether specific data protection regimes, as, for example, Title V of the Naples II Convention, should be retained. The Presidency proposes to revert to this question at the end of the second reading.

Article 15

Transfer to competent authorities in third countries or to international bodies[57]

1. Member States shall provide that personal data [received from or made available by the competent authority of another Member State][58] are not [further] transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met.

   (a) The transfer is provided for by law (...).

   (b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties or for the purpose of the prevention of threats to public security or to a person, [except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject][59].

   (c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.

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

---

[57] Reservation by CH, DE, DK, IE, NO, SE and COM. Scrutiny reservation by GR, IT and NL.

[58] The Presidency is of the opinion that the proposed DPFD regime for the exchange of data with third countries should apply to all, including purely domestic, data, should it be decided that scope of the Framework Decision is to encompass these data. It has therefore put these words between square brackets. The following delegations would prefer the scope of Article 15 to be restricted to data received from another Member State: CH, CZ, DE, DK, IE, NO, SE and UK.

[59] FR scrutiny reservation on the language between square brackets.

2. Member States shall ensure that the adequacy of the level of protection afforded by a third country or international body shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment shall result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third country or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer. It may be established that a third country or international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals

3. The Member States shall inform each other (...) of cases where they consider that a third country or an international body does not ensure an adequate level of protection within the meaning of paragraph 2.

4. (...)

5. (...)

6. By way of derogation from paragraphs 1(d) and (2) , personal data [received from the competent authority of another Member State] [60] may be [further] transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order:

   (a) to safeguard the essential interests of a Member State; or

   (b) for the prevention of imminent serious danger threatening public security or a specific person or persons; or

[60] The Presidency is of the opinion that the proposed DPFD regime for the exchange of data with third countries should apply to all, including purely domestic, data, should it be decided that scope of the Framework Decision is to encompass these data. It has therefore put these words between square brackets.

(c) the data subject has given his consent to the proposed transfer; or

[(d) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(e) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or[61]]

(f) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or[62]

(g) the transfer is necessary in order to safeguard the vital interests of the data subject.

7. (...)[63].

Article 17

Exceptions from Article 15

(...)[64].

---

[61] Reservation by AT, BE, COM, DE, DK, ES, FR, GR, HU, NL and PT. The Presidency has, for the time being, put the text between square brackets, pending the provision, by the UK delegation, of further explanation as to why it deems these exceptions are necessary.

[62] AT scrutiny reservation.

[63] At the request of several delegations, this paragraph has been replaced and is now in Article 34.

[64] This question of the relationship of this Framework Decision to other, more specific data protection provisions, should be dealt with in a more general way, in Article 34.

Article 18

Information on request of the competent authority

The receiving Member State can, in the cases referred to in Article 11(2) and (2a)[65], be requested by the competent authority from or by whom personal data were received or made available to give information about their use and further processing.

[65] Further to the comments by some delegations that this provision was worded too broadly, the Presidency proposes to restrict its scope to the cases in which a prior consent is required for further processing or certain conditions need to be complied with.

CHAPTER IV
RIGHTS OF THE DATA SUBJECT

Article 19

Obligation to provide information[66]

1. Member States shall provide that the controller or his representative must upon request provide a data subject from whom data relating to himself are collected with his knowledge with the information listed in paragraph 1(b), free of cost.

1a.[67] Where the data have not been obtained from the data subject or have been obtained from him without his knowledge or without his awareness that data are being collected concerning him, Member States shall provide that the controller or his representative must, at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, within a reasonable time after the data are first disclosed, provide the data subject with at least the information listed in paragraph 1(b), free of cost. This obligation shall apply only when, having regard to the specific circumstances in which the data are collected, the provision of further information is necessary to guarantee fair processing in respect of the data subject. It shall not apply when the data subject already has it, the provision of the information proves impossible or would involve a disproportionate effort[68], or when one of the grounds of refusal of paragraph 2 applies.

---

[66] Reservation by CZ, DE, IT, NL and NO. Scrutiny reservation by FR and PT. CZ, DK, IE, IT, NL and NO pleaded in favour of the deletion of Article 19. AT, DE, ES, FR, GR, HU and SI thought it should be retained in one form or another.

[67] DE and COM pleaded in favour of reinstating paragraph 1a in a separate Article 20.

[68] MT would prefer to use the wording 'where practicable' instead of the reference to a disproportionate effort.

1b. The following information shall be provided:

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

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

(c) the existence of the right of access to and the right to rectify the data concerning him or her.

2. The provision of the information laid down in paragraph 1b shall be refused or restricted only if necessary:

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

(b) to avoid prejudicing of investigations, inquiries or proceedings, or

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

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

(e) to protect the personal safety of individuals

[except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject][69].

[69] CZ, FR, NL and PT scrutiny reservations on the final phrase. The language was copied from Article 7(f) of the Data Protection Directive.

Article 21

Right of access, rectification, erasure or blocking[70]

1. Member States shall guarantee every data subject or the Authority supervising the controller acting upon a request from the data subject,[71] the right to obtain, upon request, from the controller (...):

(a) without constraint and without excessive delay or expense:

– 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[72],

– communication to him in an intelligible form of the data undergoing processing;

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

(bb) as appropriate, the marking of data on request of the data subject if their accuracy is denied by the data subject and if their accuracy or inaccuracy cannot be ascertained. Such mark shall only be deleted with the consent of the data subject or on the basis of a decision of the competent court or of the competent supervisory authority[73].

---

70 BE, DE, DK, FR, IE, NO and SE scrutiny reservation.

71 New wording in order to accommodate the concerns by BE. The new text only obliges Member States to ensure that either the data subject or the supervisory authority have access to the personal data.

72 SE scrutiny reservation on the reference to recipients or categories of recipients to whom the data have been disclosed.

73 ES and NL had qualms with regard to general economy of this paragraph: the marking should take place only on the basis of a court decision, as is provided for in the Prüm Treaty.

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.

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

(a) to enable the controller to fulfil its lawful duties properly[74], or

(b) to avoid prejudicing of investigations, inquiries or proceedings, or

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

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

(e) to protect the personal safety of individuals,

[except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject][75].

3. A refusal or restriction of the rights referred to in paragraph 1 shall be set out in writing[76]. If the information referred to in paragraph 1 is refused or restricted, the controller shall inform the data subject that he may appeal to the competent supervisory authority. This right of appeal shall not apply if the national law of the Member State provides for another judicial remedy against this refusal or if the information has been refused or restricted by the competent supervisory authority itself.

---

74 HU and NL reservation.

75 ES, FR and NL queried the meaning of the final phrase. The language was copied from Article 7(f) of the Data Protection Directive.

76 Language from the original proposal reinstated at the request of COM, NL and UK.

4. The reasons for a refusal or restriction according to paragraph 2 shall not be given if their communication prejudices the purpose of the refusal. In such case the controller shall inform the data subject that he may appeal to the competent supervisory authority. This right of appeal shall not apply if the national law of the Member State provides for another judicial remedy against this decision or if the information has been refused or restricted by the competent supervisory authority itself. If the data subject lodges an appeal , the authority dealing with the appeal shall examine the appeal. This authority shall, when investigating the appeal, only inform the data subject whether the controller has acted correctly or not.

Article 22

Information to third parties following rectification, blocking or erasure

Member States shall provide that appropriate measures are taken to ensure that, in cases where the controller rectifies, blocks or erases personal data following a request, (...) suppliers and addressees of these data (...) are informed of the changes performed on the personal data, unless this proves impossible or involves a disproportionate effort[77].

[77] BE, DE, DK, FR, GR, IT, NO, PT and SE scrutiny reservation.

CHAPTER V

Confidentiality and security of processing

Article 23

Confidentiality

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

Article 24

Security[78]

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

   Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Measures shall be deemed sufficient where the effort they involve is proportionate to the objective they are designed to achieve in terms of protection.

[78] DE and FR scrutiny reservation.

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

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

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

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

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

(e) ensure that 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)[79];

(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) [80];

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

[79] UK would have preferred more aspirational language.
[80] UK would have preferred more aspirational language.

(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).] [81]

3. Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

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

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

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

[81] CZ, GR, and SE argued in favour of deletion of paragraph 2, which was considered too detailed. DE, DK, FR and NL scrutiny reservation. AT and COM pleaded in favour of its retention. It was pointed out that it is a literal copy of Article 25(2) Europol Convention. As this provision will most probably have a scope that goes well beyond that of the Europol Convention and may well include domestic data processing, the Presidency agrees that the paragraph is indeed too detailed and should therefore be deleted. It has therefore placed it between square brackets.

Article 25

Notification of the supervisory authority[82]

Member States shall provide that, under conditions and procedures to be specified by domestic law, any processing operation or set of such operations intended to serve a single purpose or several related purposes, shall be notified to the supervisory authority[83]. [This may be done by way of a register kept by the controller]. The information to be contained in such notification shall include

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

(b) the purpose or purposes of the processing;

(c) a description of the category or categories of data subject;

(d) (...)[84];

(e) the recipients or categories of recipient to whom the data have been disclosed;

(f) if known, proposed transfers of data to third countries;

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

(....).

[82] DE and PL reservation. FR thought this was too detailed.

[83] The Presidency has redrafted this provision in order to align more closely to Article 1 of the Data Protection Directive.

[84] The reference to the legal basis was deleted as common law systems may not have a statutory legal basis and there is no similar reference in Article 18 of the Data Protection Directive.

Article 26

Prior checking

1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and shall check that these processing operations are examined prior to the start thereof[85].

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

3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.

[85] CZ, DE, IE and NL reservation. FR and SE scrutiny reservation.

CHAPTER VI
JUDICIAL REMEDIES AND LIABILITY

Article 27

Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 30, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed to him by the applicable national law pursuant to this Framework Decision to the processing in question[86].

Article 28

Liability[87]

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Framework Decision is entitled to receive compensation from the controller for the damage suffered. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

---

[86] SE scrutiny reservation.

[87] BE, DE, DK, FR, IT, PT and SE scrutiny reservation.

2. However, a competent authority that received personal data from the competent authority of another Member State is liable vis-à-vis the injured party for damages caused because of the use of inaccurate[88] data. It can not disclaim its liability on the ground that it received inaccurate data from another authority. If damages are awarded by an independent court or a tribunal within the meaning of Article 6(1) of the European Convention on Human Rights against the receiving authority because of its use of inaccurate data transmitted or made available by the competent authority of another Member State, the latter shall refund in full to the receiving authority the amount paid in damages insofar as the inaccuracy of the data was the result of a failure of the latter to comply with the obligations laid down in this Framework Decision[89].

Article 29

Sanctions

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

2. (...)[90].

---

[88] Several delegations objected to the use of the concept of outdated data here: CH, CZ, DE, DK.

[89] Proposed change in order to accommodate the concerns voiced by several delegations (BE, CY, DE, DK, ES, FR, IT, MT and UK) that the liability of the providing Member States should be better and more narrowly defined. The criterion of a failure to comply with the instrument, can also be found in Article 40(2) of the Europol Convention.

[90] Further to the general criticism from delegations on this paragraph, the Presidency has deleted. Mainly two reasons were put forward by delegations to oppose the proposed obligation to provide for criminal sanctions for intentionally committed offences implying serious infringements of the DPFD. A number of delegations (CH, DK, IE, IT, NL, NO, and UK) thought it should be left to the Member States to decide in which cases criminal sanctions are needed for violations of data protection provisions. Other delegations thought such an obligation could be provided for only in well-defined cases, which was not the case in the Commission's proposal (DE, ES and FR).

CHAPTER VII

SUPERVISORY AUTHORITY AND WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Article 30

Supervisory authority[91]

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

2. Each Member State shall provide that the supervisory authorities may be[92] consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties .

3. Each authority shall in particular be endowed with[93]:

   – 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,

---

[91] Several delegations indicated that they did not want to create a new authority, but entrust the tasks listed here to an existing Data Protection Supervisory Authority. COM supported this.

[92] Made optional in order to accommodate concerns voiced by CZ, FR, IE, IT and NO. COM thought the previous text already allowed for some flexibility.

[93] CZ scrutiny reservation. CH and DE thought these powers should be alternative and not cumulative. IT queried the nature of the 'investigative powers' referred to. The Presidency sees no reason to change this wording, which is copied from Article 28 of the Data Protection Directive.

– effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 26[94], and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

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

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

4. Each supervisory authority shall hear claims lodged by any person concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim, or where applicable, of the fact that a check has taken place[95].

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

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

---

94 Obviously, this power will depend on whether the mechanism currently provided for in Article 26 will be retained.

95 Language inspired by Article 28(4) of the Data Protection Directive. This modification aims at avoiding the impression that a complete information on the follow up of the claim is necessary. In most of the cases, the only information which will be communicated to the subject is that the check has taken place.

7. The supervisory authorities shall cooperate with one another as well as with the supervisory bodies set up under Title VI of the Treaty on European Union and the European Data Protection Supervisor to the extent necessary for the performance of their duties, in particular by exchanging all useful information[96].

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

9. The powers of the supervisory authority shall not extend to the judiciary acting in its judicial capacity[97].

---

[96] AT asked for the deletion of this paragraph. FR and SE likewise queried its meaning and/or legal base.

[97] Various Member States thought that the judicial independence did not need mentioning, but the Presidency, further to the suggestion of the EDPS (see para. 43 of 16050/05 CRIMORG 160 DROIPEN 64 ENFOPOL 185 DATAPROTECT 8 COMIX 864), ES and CH, inserted this new wording. This is inspired by Article 46(c) of Regulation 45/2001 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies. AT, whilst acknowledging that the independence of the judiciary made it impossible for the supervisory authority to control judicial data processing, thought some kind of 'internal judicial' control over judicial data processing should be provided for. The Presidency, like FR, submits that this is a matter which should be left to Member States.

Article 31

Working Party on the Protection of Individuals with regard to the Processing of Personal Data for the purpose of the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties

1. The Working Party on the Protection of Individuals with regard to the Processing of Personal Data set up under Article 29 of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data may be asked to give advice on matters referred to in this Framework Decision by its chairperson, either on his own initiative or at the request of a representative of the supervisory authorities, the Commission, the European Data Protection Supervisor or the chairpersons of the joint supervisory bodies[98].

   The Working Party shall be composed of a representative of the supervisory authority or authorities designated by each Member State, of a representative of the European Data Protection Supervisor, and of a representative of the Commission.

   Each member of the Working Party shall be designated by the institution, authority or authorities which he represents. Where a Member State has designated more than one supervisory authority, they shall nominate a joint representative.

   The chairpersons of the joint supervisory bodies set up under Title VI of the Treaty on European Union shall be entitled to participate or to be represented in meetings of the Working Party. The supervisory authority or authorities designated by Iceland, Norway and Switzerland shall be entitled to be represented in meetings of the Working Party insofar as issues related to the Schengen Acquis are concerned.

[98] The vast majority of delegations (CZ, DE, DK, ES, FR, NL, NO and SE) opposed the setting up of a new Working Party, as proposed by the Commission. Whilst the Presidency agrees with BE and HU that the Commission's proposal does not fall under comitology, it thinks that matters could be simplified by simply extending the mandate of the current 'Article 29 Working Party'.

2. The Working Party shall,

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

(b) give an opinion on the level of protection in the Member States and in third countries and international bodies, in particular in order to guarantee that personal data are transferred in compliance with Article 15 of this Framework Decision to third countries or international bodies that ensure an adequate level of data protection[99],

(c) advise the Commission and the Member States on any proposed amendment of this Framework Decision, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties and on any other proposed measures affecting such rights and freedoms.

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

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

---

[99] Whether and to which extent this task will be retained for the Working Party will of course hinge on the outcome of the discussions on the data protection regime to be adopted for the exchange of law enforcement data with third countries.

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

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

7. The Working Party shall draw up an annual report on the situation regarding the protection of natural persons with regard to the processing of personal data for the purpose of the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties in the European Union and in third countries, which it shall transmit to the Commission, the European Parliament and the Council. The report shall be made public.

CHAPTER VIII

Final provisions

Article 33

Amendment of the Schengen Convention

For the purposes of matters falling within the scope of the EU Treaty, this Framework Decision replaces Articles 126 to 130 of the Schengen Convention[100].

Article 34

Relation to other instruments concerning the processing and protection of personal data[101]

1. This Framework Decision replaces Article 23 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union[102].

2. Any reference to the Convention No 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data shall be construed as a reference to this Framework Decision[103].

---

100 Scrutiny reservation by BE, CH, DE, DK, GR, IT, NL and SK. It was generally agreed that Articles 34 and 35 should be reverted too at a later stage. AT and DK queried why this provision focused on Schengen.

101 AT indicated it did not want to replace the (data protection provisions of the) Prüm Treaty.

102 BE, CH, CZ, DE, ES, GR, FR, IT, NL, SK and SE scrutiny reservation. NL wants to retain Article 23. CH referred to its declaration on Article 23 that it had under the Schengen Agreement and the content of which it wanted to safeguard.

103 HU thought this reference should encompass the Council of Europe Recommendations on data protection. AT and DE indicated that some aspects of the 1981 Data Protection Convention might not be covered by the Framework Decision (e.g. the exchange of data with third countries).

3. This Framework Decision is without prejudice to any obligations and commitments incumbent upon Member States by virtue of bilateral and/or multilateral agreements with third countries concluded before the adoption of this Framework Decision.

Article 35

Implementation

1. Member States shall take the necessary measures to comply with this Framework Decision on [...][104].

2. By the same date Member States shall transmit to the General Secretariat of the Council and to the Commission the text of the provisions transposing into national law the obligations imposed on them under this Framework Decision, as well as information on the designation of the supervisory authority or authorities referred to in Article 29. 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 36

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

---

[104] Two years after adoption.