III

*(Preparatory Acts)*

# MEMBER STATES' INITIATIVES

# COUNCIL

## Initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden, with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

(2007/C 71/13)

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 30(1)(a) and (b), Article 31(1)(a), Article 32 and Article 34(2)(c) thereof,

On the initiative of the Kingdom of Belgium, the Republic of Bulgaria, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands, the Republic of Austria, the Republic of Slovenia, the Slovak Republic, the Italian Republic, the Republic of Finland, the Portuguese Republic, Romania and the Kingdom of Sweden,

Having regard to the Opinion of the European Parliament [1],

Whereas:

(1) The Council of the European Union attaches fundamental importance to the establishment of an area of freedom, security and justice, which is a fundamental concern of the people of the States brought together in the Union.

(2) The European Union has set itself the goal of giving the citizens in that area of freedom, security and justice a high degree of security by developing common procedures among the Member States in the field of police and judicial cooperation in criminal matters.

(3) The conclusions of the European Council meeting in Tampere in October 1999 confirmed the need for improved exchange of information between the competent authorities of the Member States for the purpose of detecting and investigating offences.

(4) In the Hague Programme for strengthening freedom, security and justice in the European Union of November 2004, the European Council set forth its conviction that for that purpose an innovative approach to the cross-border exchange of law enforcement information was needed.

(5) The European Council accordingly stated that the exchange of such information should comply with the conditions applying to the principle of availability. This means that a law enforcement officer in one Member State of the Union who needs information in order to carry out his duties can obtain it from another Member State and that the law enforcement agencies in the Member State that holds this information will make it available for the declared purpose, taking account of the needs of investigations pending in that Member State.

(6) The European Council set 1 January 2008 as the deadline for achieving this objective in the Hague Programme.

(7) The Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union [2] lays down rules whereby the Member States' law enforcement authorities may exchange existing information and intelligence expeditiously and effectively for the purpose of carrying out criminal investigations or criminal intelligence operations.

[1] Opinion of … (not yet published in the Official Journal).

[2] OJ L 386, 29.12.2006, p. 89.

(8) The Hague Programme for strengthening freedom, security and justice states, however, that full use should be made of new technology and that there should also be reciprocal access to national databases. The Hague Programme also stipulates that new centralised European databases should be created only on the basis of studies that have shown their added value.

(9) For effective international cooperation it is of fundamental importance that precise information can be exchanged swiftly and efficiently. The aim is to introduce procedures for promoting fast, efficient and inexpensive means of data exchange. For the joint use of data these procedures shall be subject to accountability and incorporate appropriate guarantees as to the accuracy and security of the data during transmission and storage as well as procedures for recording data exchange and restrictions on the use of information exchanged.

(10) These requirements are satisfied by the Prüm Treaty of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration. In order that the substantive requirements of the Hague Programme can be fulfilled for all Member States and that its targets in terms of time-scale can be achieved, the essential parts of the Prüm Treaty need to be made applicable to all Member States. This Council Decision should therefore be based on the main provisions of the Prüm Treaty.

(11) This Decision should therefore contain provisions designed to improve the exchange of information, whereby Member States grant one another access rights to their automated DNA analysis files, automated dactyloscopic identification systems and vehicle registration data. In the case of data from national DNA analysis files and automated dactyloscopic identification systems, a hit/no hit system should enable the searching Member State to request specific related personal data from the Member State administering the file and, where necessary, to request further information through mutual assistance procedures.

(12) This would considerably speed up existing procedures by enabling Member States to find out whether any other Member State, and if so, which, has the information it requires.

(13) Cross-border data comparison should open up a new dimension in crime fighting. The information obtained by comparing data should open up new investigative approaches for Member States and thus play a crucial role in assisting Member States' law enforcement agencies.

(14) The rules should be based on networking Member States' national databases and should thus constitute a simple and effective approach to tackling cross-border crime.

(15) Subject to certain conditions, Member States should be able to supply personal and non-personal data in order to improve the exchange of information in connection with major events with a cross-border dimension.

(16) As international cooperation, particularly in combating cross-border crime, is to be further improved, this Decision, in addition to improving the exchange of information, should allow, amongst other things, closer cooperation between police authorities, for example by means of joint security operations (e.g. joint patrols) and cross-border intervention in the event of immediate danger to life or limb.

(17) Closer police and judicial cooperation in criminal matters must go hand in hand with respect for fundamental rights, in particular the right to privacy and to protection of personal data. This should be guaranteed in this Decision by comprehensive special data protection arrangements, which should be tailored to the specific nature of the data exchange it regulates. The specific data protection provisions of the Decision should take particular account of the specific nature of cross-border on-line access to databases. Since, with on-line access, it is not possible for the Member State administering the file to make any prior checks, this Decision should ensure that post hoc monitoring takes place.

(18) Aware of the importance which this Decision has for protecting the rights of individuals, and aware that the supply of personal data to another Member State requires a sufficient standard of data protection on the part of the receiving Member State, Member States should provide for efficient implementation of all data protection rules contained in the Decision.

(19) Since the objectives of this Decision, in particular the improvement of information exchange in the European Union, cannot be sufficiently achieved by the Member States in isolation owing to the cross-border nature of crime fighting and security issues, and the Member States are forced to rely on one another in these matters, and can therefore be better achieved at European Union level, the Council may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the EC Treaty, to which Article 2 of the EU Treaty refers. In accordance with the principle of proportionality pursuant to Article 5 of the EC Treaty, this Decision does not go beyond what is necessary to achieve those objectives.

(20) This Decision respects the fundamental rights and observes the principles set out in particular in the Charter of Fundamental Rights of the European Union,

HAS DECIDED AS FOLLOWS:

CHAPTER 1

**GENERAL ASPECTS**

*Article 1*

**Aim and scope**

By means of this Decision, the Member States intend to step up cross-border cooperation in matters covered by Title VI of the EU Treaty, particularly the exchange of information between agencies responsible for the prevention and investigation of criminal offences. To this end, this Decision contains rules in the following areas:

(a) Provisions on the conditions and procedure for the automated transfer of DNA profiles, dactyloscopic data and certain national vehicle registration data (Chapter 2);

(b) Provisions on the conditions for the supply of data in connection with major events with a cross-border dimension (Chapter 3);

(c) Provisions on the conditions for the supply of information in order to prevent terrorist offences (Chapter 4);

(d) Provisions on the conditions and procedure for stepping up border police cooperation through various measures (Chapter 5).

CHAPTER 2

**ON-LINE ACCESS AND FOLLOW-UP REQUESTS**

*SECTION 1*

***DNA Profiles***

*Article 2*

**Establishment of national DNA analysis files**

1. Member States shall open and keep national DNA analysis files for the investigation of criminal offences. Processing of data kept in those files, under this Decision, shall be carried out in accordance with this Decision, in compliance with the national law applicable to the processing.

2. For the purpose of implementing this Decision, the Member States shall ensure the availability of reference data from their national DNA analysis files as referred to in the first sentence of paragraph 1. Reference data shall only include DNA profiles established from the non-coding part of DNA and a reference number. Reference data shall not contain any data from which the data subject can be directly identified. Reference data which is not attributed to any individual ('unidentified DNA-profiles') shall be recognisable as such.

3. Each Member State shall inform the General Secretariat of the Council of the national DNA analysis files to which Articles 2 to 6 apply and the conditions for automated searching as referred to in Article 3(1) in accordance with Article 33.

*Article 3*

**Automated searching of DNA profiles**

1. For the investigation of criminal offences, Member States shall allow other Member States' national contact points as referred to in Article 6, access to the reference data in their DNA analysis files, with the power to conduct automated searches by comparing DNA profiles. Searches may be conducted only in individual cases and in compliance with the requesting Member State's national law.

2. Should an automated search show that a DNA profile supplied matches DNA profiles entered in the receiving Member State's searched file, the national contact point of the receiving Member State shall receive automated notification of the reference data with which a match has been found. If no match can be found, automated notification of this shall be given.

*Article 4*

**Automated comparison of DNA profiles**

1. For the investigation of criminal offences, the Member States shall, by mutual consent, via their national contact points, compare the DNA profiles of their unidentified DNA-profiles with all DNA profiles from other national DNA analysis files' reference data. Profiles shall be supplied and compared in automated form. Unidentified DNA profiles shall be supplied for comparison only where provided for under the requesting Member State's national law.

2. Should a Member State, as a result of the comparison referred to in paragraph 1, find that any DNA profiles supplied match any of those in its DNA analysis files, it shall, without delay, supply the other Member State's national contact point with the reference data with which a match has been found.

*Article 5*

**Supply of further personal data and other information**

Should the procedures referred to in Articles 3 and 4 show a match between DNA profiles, the supply of any available further personal data and other information relating to the reference data shall be governed by the national law, including the legal assistance rules, of the requested Member State.

*Article 6*

**National contact point and implementing measures**

1. For the purposes of the supply of data as referred to in Articles 3 and 4, each Member State shall designate a national contact point. The powers of the national contact points shall be governed by the applicable national law.

2. Details of technical arrangements for the procedures set out in Articles 3 and 4 shall be laid down in the implementing measures as referred to in Article 34.

*Article 7*

**Collection of cellular material and supply of DNA profiles**

Where, in ongoing investigations or criminal proceedings, there is no DNA profile available for a particular individual present within a requested Member State's territory, the requested Member State shall provide legal assistance by collecting and examining cellular material from that individual and by supplying the DNA profile obtained, if:

(a) the requesting Member State specifies the purpose for which this is required;

(b) the requesting Member State produces an investigation warrant or statement issued by the competent authority, as required under that Member State's law, showing that the requirements for collecting and examining cellular material would be fulfilled if the individual concerned were present within the requesting Member State's territory; and

(c) under the requested Member State's law, the requirements for collecting and examining cellular material and for supplying the DNA profile obtained are fulfilled.

*SECTION 2*

***Dactyloscopic data***

*Article 8*

**Dactyloscopic data**

For the purpose of implementing this Decision, Member States shall ensure the availability of reference data from the file for the national automated fingerprint identification systems established for the prevention and investigation of criminal offences. Reference data shall only include dactyloscopic data and a reference number. Reference data shall not contain any data from which the data subject can be directly identified. Reference data which is not attributed to any individual ('unidentified dactyloscopic data') must be recognisable as such.

*Article 9*

**Automated searching of dactyloscopic data**

1. For the prevention and investigation of criminal offences, Member States shall allow other Member States' national contact points, as referred to in Article 11, access to the reference data in the automated fingerprint identification systems which they have established for that purpose, with the power to conduct automated searches by comparing dactyloscopic data. Searches may be conducted only in individual cases and in compliance with the requesting Member State's national law.

2. The confirmation of a match of dactyloscopic data with reference data held by the Member State administering the file shall be carried out by the national contact point of the requesting Member State by means of the automated supply of the reference data required for a clear match.

*Article 10*

**Supply of further personal data and other information**

Should the procedure referred to in Article 9 show a match between dactyloscopic data, the supply of any available further personal data and other information relating to the reference data shall be governed by the national law, including the legal assistance rules, of the requested Member State.

*Article 11*

**National contact point and implementing measures**

1. For the purposes of the supply of data as referred to in Article 9, each Member State shall designate a national contact point. The powers of the national contact points shall be governed by the applicable national law.

2. Details of technical arrangements for the procedure set out in Article 9 shall be laid down in the implementing measures as referred to in Article 34.

*SECTION 3*

***VEHICLE REGISTRATION DATA***

*Article 12*

**Automated searching of vehicle registration data**

1. For the prevention and investigation of criminal offences and in dealing with other offences coming within the jurisdiction of the courts or the public prosecution service in the searching Member State, as well as in maintaining public order and security, Member States shall allow other Member States' national contact points, as referred to in paragraph 2, access to the following national vehicle registration data, with the power to conduct automated searches in individual cases:

(a) data relating to owners or operators; and

(b) data relating to vehicles.

Searches may be conducted only with a full chassis number or a full registration number. Searches may be conducted only in compliance with the searching Member State's national law.

2. For the purposes of the supply of data as referred to in paragraph 1, each Member State shall designate a national contact point for incoming requests. The powers of the national contact points shall be governed by the applicable national law. Details of technical arrangements for the procedure shall be laid down in the implementing measures as referred to in Article 34.

CHAPTER 3

**MAJOR EVENTS**

*Article 13*

**Supply of non-personal data**

For the prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension, in particular for sporting events or European Council meetings, Member States shall, both upon request and of their own accord, in compliance with the supplying Member State's national law, supply one another with any non-personal data required for those purposes.

*Article 14*

**Supply of personal data**

1. For the prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension, in particular for sporting events or European Council meetings, Member States shall, both upon request and of their own accord, supply one another with personal data if any final convictions or other circumstances give reason to believe that the data subjects will commit criminal offences at the event or pose a threat to public order and security, in so far as the supply of such data is permitted under the supplying Member State's national law.

2. Personal data may be processed only for the purposes laid down in paragraph 1 and for the specified event for which they were supplied. The data supplied must be deleted without delay once the purposes referred to in paragraph 1 have been achieved or can no longer be achieved. The data supplied must in any event be deleted after not more than a year.

*Article 15*

**National contact point**

For the purposes of the supply of data as referred to in Articles 13 and 14, each Member State shall designate a national contact point. The powers of the national contact points shall be governed by the applicable national law.

CHAPTER 4

**MEASURES TO PREVENT TERRORIST OFFENCES**

*Article 16*

**Supply of information in order to prevent terrorist offences**

1. For the prevention of terrorist offences, Member States may, in compliance with national law, in individual cases, even without being requested to do so, supply other Member States' national contact points, as referred to in paragraph 3, with the personal data and information specified in paragraph 2, in so far as is necessary because particular circumstances give reason to believe that the data subjects will commit criminal offences as referred to in Articles 1 to 3 of EU Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism ([1]).

2. The data to be supplied shall comprise surname, first names, date and place of birth and a description of the circumstances giving rise to the belief referred to in paragraph 1.

([1]) OJ L 164, 22.6.2002, p. 3.

3. Each Member State shall designate a national contact point for exchange of information with other Member States' national contact points. The powers of the national contact points shall be governed by the applicable national law.

4. The supplying Member State may, in compliance with national law, impose conditions on the use made of such data and information by the receiving Member State. The receiving Member State shall be bound by any such conditions.

CHAPTER 5

**OTHER FORMS OF COOPERATION**

*Article 17*

**Joint operations**

1. In order to step up police cooperation, the competent authorities designated by the Member States may, in maintaining public order and security and preventing criminal offences, introduce joint patrols and other joint operations in which designated officers or other officials ('officers') from other Member States participate in operations within a Member State's territory.

2. Each Member State may, as a host Member State, in compliance with its own national law, and with the seconding Member State's consent, confer executive powers on the seconding Member States' officers involved in joint operations or, in so far as the host Member State's law permits, allow the seconding Member States' officers to exercise their executive powers in accordance with the seconding Member State's law. Such executive powers may be exercised only under the guidance and, as a rule, in the presence of officers from the host Member State. The seconding Member States' officers shall be subject to the host Member State's national law. The host Member State shall assume responsibility for their actions.

3. Seconding Member States' officers involved in joint operations shall be subject to the instructions given by the host Member State's competent authority.

4. Member States shall submit declarations as referred to in Article 33 in which they lay down the practical aspects of cooperation.

*Article 18*

**Assistance in connection with mass gatherings and serious accidents**

Member States' competent authorities shall provide one another with mutual assistance, in compliance with national law, in connection with mass gatherings and similar major events, and serious accidents, by seeking to prevent criminal offences and maintain public order and security by:

(a) notifying one another as promptly as possible of such situations with a cross-border impact and exchanging any relevant information;

(b) taking and coordinating the necessary policing measures within their territory in situations with a cross-border impact;

(c) as far as possible, dispatching officers, specialists and advisers and supplying equipment, at the request of the Member State within whose territory the situation has arisen.

*Article 19*

**Use of arms, ammunition and equipment**

1. Officers from a seconding Member State who are involved in a joint operation within another Member State's territory may wear their own national uniforms there. They may carry such arms, ammunition and equipment as they are allowed to under the seconding Member State's national law. The host Member State may prohibit the carrying of particular arms, ammunition or equipment by a seconding Member State's officers.

2. Member States shall submit declarations as referred to in Article 33 in which they list the arms, ammunition and equipment that may be used only in legitimate self-defence or in the defence of others. The host Member State's officer in actual charge of the operation may in individual cases, in compliance with national law, give permission for arms, ammunition and equipment to be used for purposes going beyond those specified in the first sentence. The use of arms, ammunition and equipment shall be governed by the host Member State's law. The competent authorities shall inform one another of the arms, ammunition and equipment permitted and of the conditions for their use.

3. If officers from a Member State make use of vehicles in action under this Decision within another Member State's territory, they shall be subject to the same road traffic regulations as the host Member State's officers, including as regards right of way and any special privileges.

4. Member States shall submit declarations as referred to in Article 33 in which they lay down the practical aspects of the use of arms, ammunition and equipment.

*Article 20*

**Protection and assistance**

Member States shall be required to provide other Member States' officers crossing borders with the same protection and assistance in the course of those officers' duties as for their own officers.

*Article 21*

**General rules on civil liability**

1. Where officials of a Member State are operating in another Member State, their Member State shall be liable for any damage caused by them during their operations, in accordance with the law of the Member State in whose territory they are operating.

2. The Member State in whose territory the damage referred to in paragraph 1 was caused shall make good such damage under the conditions applicable to damage caused by its own officials.

3. The Member State whose officials have caused damage to any person in the territory of another Member State shall reimburse the latter in full any sums it has paid to the victims or persons entitled on their behalf.

4. Without prejudice to the exercise of its rights vis-à-vis third parties and with the exception of paragraph 3, each Member State shall refrain, in the case provided for in paragraph 1, from requesting reimbursement of damages it has sustained from another Member State.

*Article 22*

**Criminal liability**

Officers operating within another Member State's territory under this Decision, shall be treated in the same way as officers of the host Member State with regard to any criminal offences that might be committed by, or against them, save as otherwise provided in another agreement which is binding on the Member States concerned.

*Article 23*

**Employment relationship**

Officers operating within another Member State's territory, under this Decision, shall remain subject to the employment law provisions applicable in their own Member State, particularly as regards disciplinary rules.

CHAPTER 6

**GENERAL PROVISIONS ON DATA PROTECTION**

*Article 24*

**Definitions and scope**

1. For the purposes of this Chapter:

(a) 'processing of personal data' 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, sorting, retrieval, consultation, use, disclosure by supply, dissemination or otherwise making available, alignment, combination, blocking, erasure or destruction of data. Processing within the meaning of this Decision shall also include notification of whether or not a hit exists;

(b) 'automated search procedure' shall mean direct access to the automated files of another body where the response to the search procedure is fully automated;

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

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

2. The following provisions shall apply to data which are or have been supplied pursuant to this Decision, save as otherwise provided in the preceding Chapters.

*Article 25*

**Level of data protection**

1. As regards the processing of personal data which are or have been supplied pursuant to this Decision, each Member State shall guarantee a level of protection of personal data in its national law at least equal to that resulting from the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and its Additional Protocol of 8 November 2001 and in doing so, shall take account of Recommendation No R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe to the Member States regulating the use of personal data in the police sector, also where data are not processed automatically.

2. The supply of personal data provided for under this Decision may not take place until the provisions of this Chapter have been implemented in the national law of the territories of the Member States involved in such supply. The Council shall unanimously decide whether the conditions have been met.

3. Paragraph 2 shall not apply to those Member States where the supply of personal data as provided for in this Decision has already started pursuant to the Treaty of 27 May 2005 between the Kingdom of Belgium, the Federal Republic of Germany, the Kingdom of Spain, the French Republic, the Grand Duchy of Luxembourg, the Kingdom of the Netherlands and the Republic of Austria on the stepping up of cross-border cooperation, in particular in combating terrorism, cross-border crime and illegal migration ('Prüm Treaty').

*Article 26*

**Purpose**

1. Processing of personal data by the receiving Member State shall be permitted solely for the purposes for which the data have been supplied in accordance with this Decision. Processing for other purposes shall be permitted solely with the prior authorisation of the Member State administering the file and subject only to the national law of the receiving Member State. Such authorisation may be granted provided that processing for such other purposes is permitted under the national law of the Member State administering the file.

2. Processing of data supplied pursuant to Articles 3, 4 and 9 by the receiving Member State shall be permitted solely in order to:

(a) establish whether the compared DNA profiles or dactyloscopic data match;

(b) prepare and submit a police or judicial request for legal assistance in compliance with national law if those data match;

(c) record within the meaning of Article 30.

The Member State administering the file may process the data supplied to it in accordance with Articles 3, 4 and 9 solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording pursuant to Article 30. The supplied data shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned under points (b) and (c) of the first subparagraph.

3. Data supplied in accordance with Article 12 may be used by the Member State administering the file solely where this is necessary for the purpose of providing automated replies to search procedures or recording as specified in Article 30. The data supplied shall be deleted immediately following automated replies to searches unless further processing is necessary for recording pursuant to Article 30. The receiving Member State may use data received in a reply solely for the procedure for which the search was made.

*Article 27*

**Competent authorities**

Personal data supplied may be processed only by the authorities, bodies and courts with responsibility for a task in furtherance of the aims mentioned in Article 26. In particular, data may be supplied to other entities only with the prior authorisation of the supplying Member State and in compliance with the law of the receiving Member State.

*Article 28*

**Accuracy, current relevance and storage time of data**

1. The Member States shall ensure the accuracy and current relevance of personal data. Should it transpire, including from a notification by the data subject or otherwise, that incorrect data or data which should not have been supplied have been supplied, this shall be notified without delay to the receiving Member State or Member States. The Member State or Member States concerned shall be obliged to correct or delete the data. Moreover, personal data supplied shall be corrected if they are found to be incorrect. If the receiving body has reason to believe that the supplied data are incorrect or should be deleted the supplying body shall be informed forthwith.

2. Data, the accuracy of which the data subject contests and the accuracy or inaccuracy of which cannot be established shall, in accordance with the national law of the Member States, be marked with a flag at the request of the data subject. If a flag exists, this may be removed subject to the national law of the Member States and only with the permission of the data subject or based on a decision of the competent court or independent data protection authority.

3. Personal data supplied which should not have been supplied or received shall be deleted. Data which are lawfully supplied and received shall be deleted:

(a) if they are not or no longer necessary for the purpose for which they were supplied; if personal data have been supplied and were not requested, the receiving body shall immediately check if they are necessary for the purposes for which they were supplied;

(b) following the expiry of the maximum period for keeping data laid down in the national law of the supplying Member State where the supplying body informed the receiving body of those maximum periods at the time of supplying the data.

Where there is reason to believe that deletion would prejudice the interests of the data subject, the data shall be blocked instead of being deleted in compliance with national law. Blocked data may be supplied or used solely for the purpose which prevented their deletion.

*Article 29*

**Technical and organisational measures to ensure data protection and data security**

1. The supplying and receiving bodies shall take steps to ensure that personal data is effectively protected against accidental or unauthorised destruction, accidental loss, unauthorised access, unauthorised or accidental alteration and unauthorised disclosure.

2. The specific features of the technical specification of the automated search procedure are regulated in the implementing measures as referred to in Article 34 which guarantee that:

(a) state-of-the-art technical measures are taken to ensure data protection and data security, in particular data confidentiality and integrity;

(b) encryption and authorisation procedures recognised by the competent authorities are used when having recourse to generally accessible networks; and

(c) the admissibility of searches in accordance with Article 30 (2), (4) and (5) can be checked.

*Article 30*

**Logging and recording; special rules governing automated and non-automated supply**

1. Each Member State shall guarantee that every non-automated supply and every non-automated receipt of personal data by the body administering the file and by the receiving body is logged in order to verify the admissibility of the supply. Logging shall contain the following information:

(a) the reason for the supply;

(b) the data supplied;

(c) the date of the supply; and

(d) the name or reference number of the receiving body and of the body administering the file.

2. The following shall apply to automated searches for data based on Articles 3, 9, 12 and to automated comparison pursuant to Article 4:

(a) Only specially authorised officers of the national contact points may carry out automated searches or comparisons. The list of officers authorised to carry out automated searches or comparisons, shall be made available upon request to the supervisory authorities referred to in paragraph 5 and to the other Member States.

(b) Each Member State shall ensure that each supply and receipt of personal data by the body administering the file and the receiving body is recorded, including notification of whether or not a hit exists. Recording shall include the following information:

(i) the data supplied;

(ii) the date and exact time of the supply; and

(iii) the name or reference number of the receiving body and of the body administering the file.

The receiving body shall also record the reason for the search or supply as well as an identifier for the official who carried out the search and the official who ordered the search or supply.

3. The recording body shall immediately communicate the recorded data upon request to the competent data protection bodies of the relevant Member State at the latest within four weeks following receipt of the request. Recorded data may be used solely for the following purposes:

(a) monitoring data protection;

(b) ensuring data security.

4. The recorded data shall be protected with suitable measures against inappropriate use and other forms of improper use and shall be kept for two years. After the conservation period the recorded data shall be deleted immediately.

5. Responsibility for legal checks on the supply or receipt of personal data lies with the independent data protection authorities of the respective Member States. Anyone can request these bodies to check the lawfulness of the processing of data in respect of their person in compliance with national law. Independently of such requests, these bodies and the bodies responsible for recording shall carry out random checks on the lawfulness of supply, based on the files involved.

The results of such checks shall be kept for inspection for 18 months by the independent data protection authorities. After this period, they shall be immediately deleted. Each data protection body may be requested by the independent data protection authority of another Member State to exercise its powers in accordance with national law. The independent data protection authorities of the Member States shall perform the inspection tasks necessary for mutual cooperation, in particular by exchanging relevant information.

*Article 31*

**Data subjects' rights to information and damages**

1. At the request of the data subject under national law, information shall be supplied in compliance with national law to the data subject upon production of proof of his identity, without unreasonable expense, in general comprehensible terms and without unacceptable delays, on the data processed in respect of his person, the origin of the data, the recipient or groups of recipients, the intended purpose of the processing and the legal basis for the processing. Moreover, the data subject shall be entitled to have inaccurate data corrected and unlawfully processed data deleted. The Member States shall also ensure that, in the event of violation of his rights in relation to data protection, the data subject shall be able to lodge an effective complaint to an independent court or a tribunal within the meaning of Article 6(1) of the European Convention on Human Rights or an independent supervisory authority within the meaning of Article 28 of 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 [1] and that he is given the possibility to claim for damages or to seek another form of legal compensation. The detailed rules for the procedure to assert these rights and the reasons for limiting the right of access shall be governed by the relevant national legal provisions of the Member State where the data subject asserts his rights.

[1] OJ L 281, 23.11.1995, p. 31. Directive as last amended by Regulation (EC) No 1882/2003 (OJ L 284, 31.10.2003, p. 1).

2. Where a body of one Member State has supplied personal data under this Decision, the receiving body of the other Member State cannot use the inaccuracy of the data supplied as grounds to evade its liability vis-à-vis the injured party under national law. If damages are awarded against the receiving body because of its use of inaccurate transfer data, the body which supplied the data shall refund the amount paid in damages to the receiving body in full.

*Article 32*

**Information requested by the Member States**

The receiving Member State shall inform the supplying Member State of the processing of supplied data and the result obtained.

CHAPTER 7

**IMPLEMENTING AND FINAL PROVISIONS**

*Article 33*

**Declarations**

1. For the purpose of the implementation of this Decision, each Member State shall submit declarations to the General Secretariat of the Council when transmitting the text of the provisions transposing into its national law the obligations imposed on it under this Decision as referred to in Article 37 (2).

2. Declarations submitted in accordance with paragraph 1 may be amended at any time by means of a declaration submitted to the General Secretariat of the Council. The General Secretariat of the Council shall forward any declarations received to the Member States and the Commission.

*Article 34*

**Implementing measures**

The Council shall adopt measures necessary to implement this Decision at the level of the Union in accordance with the procedure laid down in the second sentence of Article 34(2)(c) of the EU Treaty.

*Article 35*

**Costs**

Each Member State shall bear the operational costs incurred by its own authorities in connection with the implementation of this Decision. In special cases, the Member States concerned may agree on different arrangements.

*Article 36*

**Relationship with other instruments**

1. Member States may continue to apply bilateral or multilateral agreements or arrangements which concern the scope of this Decision and are in force on the date it is adopted in so far as such agreements or arrangements provide for the objectives of this Decision to be extended or enlarged. For the Member States concerned, the relevant provisions of this Decision shall be applied instead of provisions concerning the scope of this Decision contained in the Prüm Treaty. Any Article or any part of an Article of the Prüm Treaty with regard to which no provision of this Decision is applied instead of the Prüm Treaty shall remain applicable between the contracting parties of the Prüm Treaty.

2. Member States may conclude or bring into force bilateral or multilateral agreements or arrangements which concern the scope of this Decision after it has entered into force in so far as such agreements or arrangements provide for the objectives of this Decision to be extended or enlarged.

3. The agreements and arrangements referred to in paragraphs 1 and 2 may not affect relations with Member States which are not parties thereto.

4. Within [… years] of this Decision taking effect Member States shall inform the Council and the Commission of existing agreements or arrangements within the meaning of paragraph 1 which they wish to continue to apply.

5. Member States shall also inform the Council and the Commission of all new agreements or arrangements within the meaning of paragraph 2 within 3 months of their signing or, in the case of instruments which were signed before adoption of this Decision, within three months of their entry into force.

6. Nothing in this Decision shall affect bilateral or multilateral agreements or arrangements between Member States and third countries.

*Article 37*

**Implementation**

1. Member States shall take the necessary measures to comply with the provisions of this Decision within [… years] of this Decision taking effect.

2. Member States shall transmit to the General Secretariat of the Council and the Commission the text of the provisions transposing into their national law the obligations imposed on them under this Decision. When doing so, each Member State may indicate that it will apply immediately this Decision in its relations with those Member States which have given the same notification.

3. On the basis of this and other information made available by Member States on request, the Commission shall submit a report to the Council by [at the latest after three years after taking effect] on the implementation of this Decision and proposals for any further development.

*Article 38*

**Application**

This Decision shall take effect [… days] following its publication in the *Official Journal of the European Union*.

Done at Brussels, on …

*For the Council*

*The President*