III

(Acts adopted under the EU Treaty)

ACTS ADOPTED UNDER TITLE VI OF THE EU TREATY

COUNCIL FRAMEWORK DECISION 2008/977/JHA

of 27 November 2008

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

THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the Commission,

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

Whereas:

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

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

(3) Legislation falling within the scope 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 the protection of personal data. Common standards regarding the processing and protection of personal data processed for the purpose of preventing and combating crime contribute to the achieving of 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 the 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 [2].

(5) The exchange of personal data within 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 rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way that excludes any discrimination in respect of such 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 [3] does not apply to the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title VI of the Treaty on European Union, nor, in any case, to processing operations concerning public security, defence, state security or the activities of the State in areas of criminal law.

[1] OJ C 125 E, 22.5.2008, p. 154.

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

[3] OJ L 281, 23.11.1995, p. 31.

(6) This Framework Decision applies only to data gathered or processed by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. This Framework Decision should leave it to Member States to determine more precisely at national level which other purposes are to be considered as incompatible with the purpose for which the personal data were originally collected. In general, further processing for historical, statistical or scientific purposes should not be considered as incompatible with the original purpose of the processing.

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

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

(9) This Framework Decision should not apply to personal data which a Member State has obtained within the scope of this Framework Decision and which originated in that Member State.

(10) 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.

(11) It is necessary to specify the objectives of data protection within 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 lawfully and in accordance with fundamental principles relating to data quality. At the same time the legitimate activities of the police, customs, judicial and other competent authorities should not be jeopardised in any way.

(12) The principle of accuracy of data is to be applied taking account of the nature and purpose of the processing concerned. For example, in particular in judicial proceedings data are based on the subjective perception of individuals and in some cases are totally unverifiable. Consequently, the requirement of accuracy cannot appertain to the accuracy of a statement but merely to the fact that a specific statement has been made.

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

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

(15) As regards inaccurate, incomplete or no longer up-to-date data transmitted or made available to another Member State and further processed by quasi-judicial authorities, meaning authorities with powers to make legally binding decisions, its rectification, erasure or blocking should be carried out in accordance with national law.

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

(17) It is appropriate to lay down at the European level the conditions under which competent authorities of the Member States should be allowed to transmit and make available personal data received from other Member States to authorities and private parties in Member States. In many cases the transmission of personal data by the judiciary, police or customs to private parties is necessary to prosecute crime or to prevent an immediate and serious threat to public security or to prevent serious harm to the rights of individuals, for example, by issuing alerts concerning forgeries of securities to banks and credit institutions, or, in the area of vehicle crime, by communicating personal data to insurance companies in order to prevent illicit trafficking in stolen motor vehicles or to improve the conditions for the recovery of stolen motor vehicles from abroad. This is not tantamount to the transfer of police or judicial tasks to private parties.

(18) The rules in this Framework Decision regarding the transmission of personal data by the judiciary, police or customs to private parties do not apply to the disclosure of data to private parties (such as defence lawyers and victims) in the context of criminal proceedings.

(19) 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.

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

(21) Where personal data may be further processed for administrative proceedings, these proceedings also include activities by regulatory and supervisory bodies.

(22) The legitimate activities of the police, customs, judicial and other competent authorities may require that data are sent to authorities in third States or international bodies that have obligations for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

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

(24) Where personal data are transferred from a Member State to third States or international bodies, such transfer should, in principle, take place only after the Member State from which the data were obtained has given its consent to the transfer. Each Member State should be able to determine the modalities of such consent, including, for example, by means of a general consent for categories of information or for specified third States.

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

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

(27) Member States should ensure that the data subject is informed that the personal data could be or are being collected, processed or transmitted to another Member State for the purpose of prevention, investigation, detection, and prosecution of criminal offences or the execution of criminal penalties. The modalities of the right of the data subject to be informed and the exceptions thereto should be determined by national law. This may take a general form, for example, through the law or through the publication of a list of the processing operations.

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

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

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

(31) 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.

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

(33) 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 within the framework of police and judicial cooperation between the Member States.

(34) The supervisory authorities already established in Member States under Directive 95/46/EC should also be able to assume responsibility for the tasks to be performed by the national supervisory authorities to be established under this Framework Decision.

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

(36) Article 47 of the Treaty on European Union stipulates that nothing in it is to 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, 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 [1] 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) [2].

(37) This Framework Decision is without prejudice to the rules pertaining to illicit access to data laid down in Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems [3].

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

(39) Several acts, adopted on the basis of Title VI of the Treaty on European Union, contain specific provisions on the protection of personal data exchanged or otherwise processed pursuant to those acts. In some cases these provisions constitute a complete and coherent set of rules covering all relevant aspects of data protection (principles of data quality, rules on data security, regulation of the rights and safeguards of data subjects, organisation of supervision and liability) and they regulate these matters in more detail than this Framework Decision. The relevant set of data protection provisions of those acts, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), as well as those introducing direct access for the authorities of Member States to certain data systems of other Member States, should not be affected by this Framework Decision. The same applies in respect of the data protection provisions governing the automated transfer between Member States of DNA profiles, dactyloscopic data and national vehicle registration data pursuant to the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime [4].

(40) In other cases the provisions on data protection in acts, adopted on the basis of Title VI of the Treaty on European Union, are more limited in scope. They often set specific conditions for the Member State receiving information containing personal data from other Member States as to the purposes for which it can use those data, but refer for other aspects of data protection to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 or to national law. To the extent that the provisions of those acts imposing conditions on receiving Member States as to the use or further transfer of personal data are more restrictive than those contained in the corresponding provisions of this Framework Decision, the former provisions should remain unaffected. However, for all other aspects the rules set out in this Framework Decision should be applied.

(41) This Framework Decision does not affect the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the Additional Protocol to that Convention of 8 November 2001 or the Council of Europe conventions on judicial cooperation in criminal matters.

[1] OJ L 8, 12.1.2001, p. 1.
[2] OJ L 201, 31.7.2002, p. 37.
[3] OJ L 69, 16.3.2005, p. 67.
[4] OJ L 210, 6.8.2008, p. 1.

(42) Since the objective of this Framework Decision, 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, and can therefore, by reason of the scale and effects of the action, be better achieved at the Union level, the Union may adopt measures in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty establishing the European Community and referred to in Article 2 of the Treaty on European Union. In accordance with the principle of proportionality as set out in Article 5 of the Treaty establishing the European Community, this Framework Decision does not go beyond what is necessary to achieve that objective.

(43) 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 Treaty on European Union and to the Treaty establishing the European Community, 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* ([1]).

(44) 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 Treaty on European Union and to the Treaty establishing the European Community, 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* ([2]).

(45) 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 latter's association with the implementation, application and development of the Schengen *acquis* ([3]), which fall within the area referred to in Article 1, points H and I of Council Decision 1999/437/EC ([4]) on certain arrangements for the application of that Agreement.

(46) As regards Switzerland, this Framework Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([5]), which fall within the area referred to in Article 1, point H and I of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/149/JHA ([6]) on the conclusion of that Agreement on behalf of the European Union.

(47) As regards Liechtenstein, this Framework Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol signed between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, which fall within the area referred to in Article 1, point H and I of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/262/JHA ([7]) on the signature of that Protocol on behalf of the European Union.

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

HAS ADOPTED THIS FRAMEWORK DECISION:

Article 1

Purpose and scope

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

2. In accordance with this Framework Decision, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy when, for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, personal data:

(a) are or have been transmitted or made available between Member States;

([1]) OJ L 131, 1.6.2000, p. 43.
([2]) OJ L 64, 7.3.2002, p. 20.
([3]) OJ L 176, 10.7.1999, p. 36.
([4]) OJ L 176, 10.7.1999, p. 31.
([5]) OJ L 53, 27.2.2008, p. 52.
([6]) OJ L 53, 27.2.2008, p. 50.
([7]) OJ L 83, 26.3.2008, p. 5.
([8]) OJ C 303, 14.12.2007, p. 1.

(b) are or have been transmitted or made available by Member States to authorities or to information systems established on the basis of Title VI of the Treaty on European Union; or

(c) are or have been transmitted or made available to the competent authorities of the Member States by authorities or information systems established on the basis of the Treaty on European Union or the Treaty establishing the European Community.

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

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

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

Article 2

Definitions

For the purposes of this Framework Decision:

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

(c) 'blocking' means the marking of stored personal data with the aim of limiting their processing in future;

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

(e) 'processor' means any body which processes personal data on behalf of the controller;

(f) 'recipient' means any body to which data are disclosed;

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

(h) 'competent authorities' mean agencies or bodies established by legal acts adopted by the Council pursuant to Title VI of the Treaty on European Union, as well as police, customs, judicial and other competent authorities of the Member States that are authorised by national law to process personal data within the scope of this Framework Decision;

(i) 'controller' means 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;

(j) 'referencing' means the marking of stored personal data without the aim of limiting their processing in future;

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

Article 3

Principles of lawfulness, proportionality and purpose

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

2. Further processing for another purpose shall be permitted in so far as:

(a) it is not incompatible with the purposes for which the data were collected;

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

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

The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous.

Article 4

Rectification, erasure and blocking

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

2. Personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed. Archiving of those data in a separate data set for an appropriate period in accordance with national law shall not be affected by this provision.

3. Personal data shall be blocked instead of erased if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Blocked data shall be processed only for the purpose which prevented their erasure.

4. When the personal data are contained in a judicial decision or record related to the issuance of a judicial decision, the rectification, erasure or blocking shall be carried out in accordance with national rules on judicial proceedings.

Article 5

Establishment of time limits for erasure and review

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

Article 6

Processing of special categories of data

The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards.

Article 7

Automated individual decisions

A decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.

Article 8

Verification of quality of data that are transmitted or made available

1. The competent authorities shall take all reasonable steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available. To that end, the competent authorities shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. As far as possible, in all transmissions of data, available information shall be added which enables the receiving Member State to assess the degree of accuracy, completeness, up-to-dateness and reliability. If personal data were transmitted without request the receiving authority shall verify without delay whether these data are necessary for the purpose for which they were transmitted.

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

Article 9

Time limits

1. Upon transmission or making available of the data, the transmitting authority may in line with the national law and in accordance with Articles 4 and 5, indicate the time limits for the retention of data, upon the expiry of which the recipient must erase or block the data or review whether or not they are still needed. This obligation shall not apply if, at the time of the expiry of these time limits, the data are required for a current investigation, prosecution of criminal offences or enforcement of criminal penalties.

2. Where the transmitting authority has not indicated a time limit in accordance with paragraph 1, the time limits referred to in Articles 4 and 5 for the retention of data provided for under the national law of the receiving Member State shall apply.

Article 10

Logging and documentation

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

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

Article 11

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

Personal data received from or made available by the competent authority of another Member State may, in accordance with the requirements of Article 3(2), be further processed only for the following purposes other than those for which they were transmitted or made available:

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

(b) other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

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

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

The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as, for example, making the data anonymous.

Article 12

Compliance with national processing restrictions

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

2. When applying paragraph 1, Member States shall not apply restrictions regarding data transmissions to other Member States or to agencies or bodies established pursuant to Title VI of the Treaty on European Union other than those applicable to similar national data transmissions.

Article 13

Transfer to competent authorities in third States or to international bodies

1. Member States shall provide that personal data transmitted or made available by the competent authority of another Member State may be transferred to third States or international bodies, only if:

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

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

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

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

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

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

(a) the national law of the Member State transferring the data so provides because of:

(i) legitimate specific interests of the data subject; or

(ii) legitimate prevailing interests, especially important public interests; or

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

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

Article 14

Transmission to private parties in Member States

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

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

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

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

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

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

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

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

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

Article 15

Information on request of the competent authority

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

Article 16

Information for the data subject

1. Member States shall ensure that the data subject is informed regarding the collection or processing of personal data by their competent authorities, in accordance with national law.

2. When personal data have been transmitted or made available between Member States, each Member State may, in accordance with the provisions of its national law referred to in paragraph 1, ask that the other Member State does not inform the data subject. In such case the latter Member State shall not inform the data subject without the prior consent of the other Member State.

Article 17

Right of access

1. Every data subject shall have the right to obtain, following requests made at reasonable intervals, without constraint and without excessive delay or expense:

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

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

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

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

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

(c) to protect public security;

(d) to protect national security;

(e) to protect the data subject or the rights and freedoms of others.

3. Any refusal or restriction of access shall be set out in writing to the data subject. At the same time, the factual or legal reasons on which the decision is based shall also be communicated to him. The latter communication may be omitted where a reason under paragraph 2(a) to (e) exists. In all of these cases the data subject shall be advised that he may appeal to the competent national supervisory authority, a judicial authority or to a court.

Article 18

Right to rectification, erasure or blocking

1. The data subject shall have the right to expect the controller to fulfil its duties in accordance with Articles 4, 8 and 9 concerning the rectification, erasure or blocking of personal data which arise from this Framework Decision. Member States shall lay down whether the data subject may assert this right directly against the controller or through the intermediary of the competent national supervisory authority. If the controller refuses rectification, erasure or blocking, the refusal must be communicated in writing to the data subject who must be informed of the possibilities provided for in national law for lodging a complaint or seeking judicial remedy. Upon examination of the complaint or judicial remedy, the data subject shall be informed whether the controller acted properly or not. Member States may also provide that the data subject shall be informed by the competent national supervisory authority that a review has taken place.

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

Article 19

Right to compensation

1. Any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Framework Decision shall be entitled to receive compensation for the damage suffered from the controller or other authority competent under national law.

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

Article 20

Judicial remedies

Without prejudice to any administrative remedy for which provision may be made prior to referral to the judicial authority, the data subject shall have the right to a judicial remedy for any breach of the rights guaranteed to him by the applicable national law.

Article 21

Confidentiality of processing

1. Any person who has access to personal data which fall within the scope of this Framework Decision may process such data only if that person is a member of, or acts on instructions of, the competent authority, unless he is required to do so by law.

2. Persons working for a competent authority of a Member State shall be bound by all the data protection rules which apply to the competent authority in question.

Article 22

Security of processing

1. Member States shall provide that the competent authorities must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission over a network or the making available by granting direct automated access, and against all other unlawful forms of processing, taking into account in particular the risks represented by the processing and the nature of the data to be protected. Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

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

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

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

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

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

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

(f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

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

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

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

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

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

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

Article 23

Prior consultation

Member States shall ensure that the competent national supervisory authorities are consulted prior to the processing of personal data which will form part of a new filing system to be created where:

(a) special categories of data referred to in Article 6 are to be processed; or

(b) the type of processing, in particular using new technologies, mechanism or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the privacy, of the data subject.

Article 24

Penalties

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 penalties to be imposed in case of infringements of the provisions adopted pursuant to this Framework Decision.

Article 25

National supervisory authorities

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

2. Each authority shall in particular be endowed with:

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

(b) effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions;

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

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

4. Member States shall provide that the members and staff of the supervisory authority are bound by the data protection provisions applicable to the competent authority in question and, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

Article 26

Relationship to agreements with third States

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

In the application of these agreements, the transfer to a third State of personal data obtained from another Member State, shall be carried out while respecting Article 13(1)(c) or (2), as appropriate.

Article 27

Evaluation

1. Member States shall report to the Commission by 27 November 2013 on the national measures they have taken to ensure full compliance with this Framework Decision, and particularly with regard to those provisions that already have to be complied with when data is collected. The Commission shall examine in particular the implications of those provisions for the scope of this Framework Decision as laid down in Article 1(2).

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

Article 28

Relationship to previously adopted acts of the Union

Where in acts, adopted under Title VI of the Treaty on European Union prior to the date of entry into force of this Framework Decision and regulating the exchange of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaty establishing the European Community, specific conditions have been introduced as to the use of such data by the receiving Member State, these conditions shall take precedence over the provisions of this Framework Decision on the use of data received from or made available by another Member State.

Article 29

Implementation

1. Member States shall take the necessary measures to comply with the provisions of this Framework Decision before 27 November 2010.

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 their national law the obligations imposed on them under this Framework Decision, as well as information on the supervisory authorities referred to in Article 25. On the basis of a report established using this information by the Commission, the Council shall, before 27 November 2011, assess the extent to which Member States have complied with the provisions of this Framework Decision.

Article 30

Entry into force

This Framework Decision shall enter into force on the 20th day following its publication in the *Official Journal of the European Union*.

Done at Brussels, 27 November 2008.

For the Council

The President

M. ALLIOT-MARIE