Protection of personal data *


(Consultation procedure)

The proposal was amended as follows (1):

<table>
<thead>
<tr>
<th>TEXT PROPOSED</th>
<th>AMENDMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>BY THE COMMISSION</td>
<td>BY PARLIAMENT</td>
</tr>
</tbody>
</table>

Amendment 1

Citation 1

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

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

Amendment 2

Recital 9

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

(9) Ensuring a high level of protection of the personal data of all persons within the territory of the European Union requires common provisions to determine the lawfulness and the quality of data processed by competent authorities in other Member States. It also requires that personal data be collected and processed for legitimate and specific purposes. Data may not be further processed in a way incompatible with those purposes, including in the framework of the increasing exchange of information between law enforcement and judicial authorities and in relation to the proposal on the interoperability of databases.

Amendment 3

Recital 12

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

(12) Where personal data are transferred from a Member State of the European Union to third countries or international bodies, these data should benefit from an adequate level of protection. This Framework Decision should ensure that personal data received from third countries comply at least with international standards on the respect of human rights.

(1) The matter was then referred back to committee pursuant to Rule 53(2) (A6-0192/2006).
Amendments 4 and 5

Recital 15

(15) It is appropriate to establish common rules on the confidentiality and security of the processing, on liability and sanctions for unlawful use by competent authorities as well as judicial remedies available for the data subject. Furthermore, it is necessary that Member States provide for criminal sanctions for particularly serious and intentionally committed infringements of data protection provisions.

(15) It is appropriate to establish common rules on the confidentiality and security of the processing, on liability and sanctions for unlawful use by competent authorities and by private parties processing personal data on behalf of competent authorities or in a public capacity, as well as judicial remedies available for the data subject. Furthermore, it is necessary that Member States provide for criminal sanctions for particularly serious and intentional or grossly negligent infringements of data protection provisions.

Amendment 6

Recital 20

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

(20) The present Framework Decision is without prejudice to the specific data protection provisions laid down in the relevant legal instruments relating to the processing and protection of personal data by Europol, Eurojust and the Customs Information System. However, at the latest two years after the date referred to in Article 35(1), the specific data protection provisions applicable to Europol, Eurojust and the Customs Information System should be made fully consistent with this Framework Decision, with a view to enhancing the consistency and effectiveness of the legal framework on data protection pursuant to a proposal by the Commission.

Amendment 7

Recital 20a (new)

(20a) Europol, Eurojust and the Customs Information System should retain those of their data protection rules which clearly provide that personal data may be processed, consulted or transmitted only on the basis of more specific and/or protective conditions or restrictions.

Amendment 8

Recital 22

(22) It is appropriate that this Framework Decision applies to the personal data which are processed in the framework of the second generation of the Schengen Information System and the related exchange of supplementary information pursuant to Decision JHA/2006/... on the establishment, operation and use of the second generation Schengen information system.

(22) It is appropriate that this Framework Decision applies to the personal data which are processed in the framework of the second generation of the Schengen Information System and the related exchange of supplementary information pursuant to Decision 2006/.../JHA of... on access for consultation purposes to the Visa Information System (VIS) by the authorities of Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (1).

(1) OJ L ...
Amendment 9
Recital 32a (new)

(32a) Having regard to the Opinion of the European Data Protection Supervisor,

Amendment 10
Article 1, paragraph 2

2. *Member States shall ensure that* the disclosure of personal data to the competent authorities of other Member States is neither restricted nor prohibited for reasons connected with the protection of personal data as provided for in this Framework Decision.

2. *This Framework Decision does not preclude Member States from providing safeguards for the protection of personal data in the context of police and judicial cooperation in criminal matters greater than those established in this Framework Decision. However, any such provisions may not restrict or prohibit the disclosure of personal data to the competent authorities of other Member States for reasons connected with the protection of personal data as provided for in this Framework Decision.*

Amendment 11
Article 3, paragraph 2a (new)

2a. *This Framework Decision shall not apply if specific legislation under Title VI of the TEU explicitly provides that personal data are to be processed, accessed or transmitted only under more specific conditions or restrictions.*

Amendment 12
Article 4, paragraph 1, point (d)

(d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. Member States may provide for the processing of data to varying degrees of accuracy and reliability in which case they must provide that data are distinguished in accordance with their degree of accuracy and reliability, and in particular that data based on facts are distinguished from data based on opinions or personal assessments.

(d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. *However*, Member States may provide for the processing of data to varying degrees of accuracy and reliability in which case they must provide that data are distinguished in accordance with their degree of accuracy and reliability, and in particular that data based on facts are distinguished from data based on opinions or personal assessments. *Member States shall provide that the quality of personal data is checked regularly. As far as possible, judicial decisions and decisions not to prosecute shall be indicated and data based on opinions or personal assessments shall be checked at source and their degree of accuracy or reliability indicated. Member States shall, without prejudice to national criminal procedure, provide that personal data are marked on request of the data subject if their accuracy is disputed by the data subject and if their accuracy or inaccuracy cannot be ascertained. Such a mark shall only be deleted with the consent of the data subject or on the basis of a decision of the competent court or of the competent supervisory authority;*
Amendment 13
Article 4, paragraph 4

4. Member States shall provide that processing of personal data is only necessary if

— there are, based on established facts, reasonable grounds to believe that the personal data concerned would make possible, facilitate or accelerate the prevention, investigation, detection or prosecution of a criminal offence, and

— there is no other means less affecting the data subject and

— the processing of the data is not excessive in relation to the offence concerned.

Amendment 14
Article 4, paragraph 4a (new)

4a. Member States shall take into account the various categories of personal data and the various purposes for which they are collected with a view to laying down time limits for their storage and appropriate conditions for their collection, further processing and transfer. Personal data relating to those who are not suspected of having committed or taken part in a criminal offence may be processed only for the purpose for which they were collected and for a limited period. Member States shall lay down appropriate limitations on access to and transmission of such data.

Amendment 15
Article 4a, paragraph 1 (new)

Article 4a

Further processing of personal data

1. Member States shall provide that personal data may be further processed only in accordance with this Framework Decision, in particular Articles 4, 5 and 6 hereof,

(a) for the specific purpose for which they were transmitted or made available,

(b) if strictly necessary, for the purpose of the prevention, investigation, detection or prosecution of serious criminal offences, or

(c) for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.
Amendment 16
Article 4 a, paragraph 2 (new)

2. The personal data concerned shall be further processed for the purposes referred to in paragraph 1(c) only with the prior consent of the authority that transmitted or made available the personal data. Member States may, subject to adequate legal safeguards, adopt legislative measures to allow such further processing.

Amendment 17
Article 5

Member States shall provide that personal data may be processed by the competent authorities only if provided for by a law setting out that the processing is necessary for the fulfilment of the legitimate task of the authority concerned and for the purpose of the prevention, investigation, detection or prosecution of criminal offences.

Member States shall, after consulting the supervisory authority established in Article 30, provide that personal data may be processed by the competent authorities only if provided for by a law setting out that the processing is necessary for the fulfilment of the legitimate task of the authority concerned and for the purpose of the prevention, investigation, detection or prosecution of criminal offences, and where

(a) the data subject has unambiguously given his consent, provided that the processing is carried out in his interest; or

(b) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(c) processing is necessary in order to protect the vital interests of the data subject.

Amendment 18
Article 5, paragraph 1a (new)

1a. Member States shall provide that personal data are processed only if:

— competent authorities can demonstrate, on the basis of established facts, a clear need to process the personal data concerned for the prevention, investigation, detection or prosecution of a criminal offence, and

— there are no other means having a less adverse effect on the data subject, and

— the processing of the data is not excessive in relation to the offence concerned.

Amendment 19
Article 6, paragraph 2, indent 1

— processing is provided for by a law and absolutely necessary for the fulfilment of the legitimate task of the authority concerned for the purpose of the prevention, investigation, detection or prosecution of criminal offences and is limited
to a particular inquiry or if the data subject has given his or her explicit consent to the processing, provided that the processing is carried out in the interest of the data subject and the data subject would not suffer adverse consequences for refusing to grant consent; and

Amendment 20
Article 6, paragraph 2a (new)

2a. Member States shall implement special technical and organisational requirements for the processing of sensitive data.

Amendment 21
Article 6, paragraph 2b (new)

2b. Member States shall provide for additional specific safeguards with regard to biometric data and DNA profiles, with a view to ensuring that:

— biometric data and DNA profiles are used only on the basis of well-established and interoperable technical standards;

— the degree of accuracy of biometric data and DNA profiles is carefully taken into account and may be challenged by the data subject through readily available means;

— the respect of the dignity and integrity of persons is fully ensured.

Amendment 22
Article 7, paragraph 1

1. Member States shall provide that personal data shall be stored for no longer than necessary for the purpose for which it was collected, unless otherwise provided by national law. Personal data of persons referred to in Article 4(3) last indent shall be stored for only as long as is absolutely necessary for the purpose for which it was collected.

1. Member States shall provide that personal data shall be stored for no longer than necessary for the purpose for which it was collected or further processed, in accordance with Article 4(1)(e) and Article 4a. Personal data of persons referred to in Article 4(3) last indent shall be stored for only as long as is absolutely necessary for the purpose for which it was collected.

Amendment 23
Article 7, paragraph 2

2. Member States shall provide for appropriate procedural and technical measures ensuring that time limits for the storage of personal data are observed. Compliance with such time limits shall be regularly reviewed.

2. Member States shall provide for appropriate procedural and technical measures ensuring that time limits for the storage of personal data are observed. Such measures shall include the automatic and regular deletion of personal data after a certain period. Compliance with such time limits shall be regularly reviewed.
Amendment 24

Chapter III, Section I, Title

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

Amendment 25

Article 8

Member States shall provide that personal data shall only be transmitted or made available to the competent authorities of other Member States if necessary for the fulfilment of a legitimate task of the transmitting or receiving authority and for the purpose of the prevention, investigation, detection or prosecution of criminal offences.

Member States shall provide that personal data collected and processed by the competent authorities shall only be transmitted or made available to the competent authorities of other Member States if necessary for the fulfilment of a legitimate task of the transmitting or receiving authority and for the purpose of the prevention, investigation, detection or prosecution of specific criminal offences.

Amendment 26

Article 8a (new)

Article 8a

Transmission to authorities other than competent authorities

Member States shall provide that personal data are transmitted to authorities of a Member State other than competent authorities only in particular individual and well-founded cases and if all the following requirements are met:

(a) the transmission is provided for by law clearly obliging or authorising it, and

(b) the transmission is necessary for the specific purpose for which the data concerned were collected, transmitted or made available or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject

or

necessary because the data concerned are indispensable to the authority to which the data are to be further transmitted to enable it to fulfil its own lawful task and provided that the aim of the collection or processing to be carried out by that authority is not incompatible with the original processing, and the legal obligations of the competent authority which intends to transmit the data are not contrary to this,

or

undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent.
Article 8b

Transmission to private parties

Member States shall, without prejudice to national criminal procedural rules, provide that personal data may be transmitted to private parties in a Member State only in specific cases and if all the following requirements are met:

(a) the transmission is provided for by a law clearly obliging or authorising it, and

(b) the transmission is necessary for the purpose for which the data concerned were collected, transmitted or made available or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject. Member States shall provide that competent authorities may have access to and process personal data controlled by private parties only on a case-by-case basis, in specified circumstances, for specified purposes and subject to judicial scrutiny in the Member States.

Article 8c

Data processing by private parties in connection with public administration

Member States shall lay down in their national legislation that, where private parties collect and process data in connection with public administration, they are subject to obligations which are either equivalent to or stricter than those imposed on competent authorities.

Article 8d

Transfer to competent authorities in third countries or to international bodies

1. Member States shall provide that personal data are not transferred to competent authorities of third countries or to international bodies except if such transfer is in compliance with this Framework Decision and, in particular, all the following requirements are met:

(a) the transfer is provided for by a law clearly obliging or authorising it;
(b) the transfer is necessary for the purpose for which the data concerned were collected, transmitted or made available or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject;

(c) an adequate level of data protection is ensured in the third country or by the international body to which the data concerned are to be transferred.

2. Member States shall ensure that the adequacy of the level of protection afforded by a third country or international body is assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment shall be based on an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third country or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer.

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

4. Where the Commission, after consulting the Council and the European Parliament, establishes that a third country or international body does not ensure an adequate level of protection within the meaning of paragraph 2, the Member States shall take the measures necessary to prevent any transfer of personal data to the third country or international body in question.

5. The Commission, after consulting the Council and the European Parliament, may establish that a third country or international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law and of the international agreements it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.

6. Exceptionally, as a derogation from paragraph 1, point (c), personal data may be transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of an imminent serious danger threatening public security or a specific person or persons. In such a case, personal data may be processed by the receiving party only insofar as they are absolutely necessary for the specific purpose for which they were transmitted. Such transfers shall be notified to the competent supervisory authority.
Amendment 30
Article 9, paragraph 6

6. Member States shall, without prejudice to national criminal procedure, provide that personal data are marked on request of the data subject if their accuracy is denied by the data subject and if their accuracy or inaccuracy cannot be ascertained. Such mark shall only be deleted with the consent of the data subject or on the basis of a decision of the competent court or of the competent supervisory authority.

Amendment 31
Article 9, paragraph 7, indent 3

— if these data are not or no longer necessary for the purpose for which they were transmitted or made available.

— and in any event if these data are not or no longer necessary for the purpose for which they were transmitted or made available.

Amendment 32
Article 9, paragraph 9a (new)

9a. Member States shall provide that the quality of personal data transmitted or made available by third countries is specifically assessed as soon as they are received and that the degree of accuracy and reliability is indicated.

Amendment 33
Article 10, paragraph 1

1. Member States shall provide that each automated transmission and reception of personal data, in particular by direct automated access, is logged in order to ensure the subsequent verification of the reasons for the transmission, the transmitted data, the time of transmission, the authorities involved and, as far as the receiving authority is concerned, the persons who have received the data and who have given rise to their reception.

2. Member States shall provide that each non automated transmission and reception of personal data is documented in order to ensure the subsequent verification of the reasons for the transmission, the transmitted data, the time of transmission, the authorities involved and, as far as the receiving authority is concerned, the persons who have received the data and who have given rise to their reception.

Amendment 34
Article 10, paragraph 2

1. Member States shall provide that each automated access, transmission and reception of personal data, in particular by direct automated access, is logged in order to ensure the subsequent verification of the reasons for the access and transmission, the transmitted or accessed data, the time of transmission or access, the authorities involved and, as far as the receiving authority is concerned, the persons who have received the data and who have given rise to their reception.

2. Member States shall provide that each non automated access, transmission and reception of personal data is documented in order to ensure the subsequent verification of the reasons for the access or transmission, the transmitted or accessed data, the time of transmission or access, the authorities involved and, as far as the receiving authority is concerned, the persons who have received the data and who have given rise to their reception.
Amendment 35
Article 10, paragraph 3

3. The authority that has logged or documented such information shall communicate it without delay to the competent supervisory authority on request of the latter. The information shall only be used for the control of data protection and for ensuring proper data processing as well as data integrity and security.

Amendment 36
Article 12a (new)

Article 12a

Further transmission to authorities other than competent authorities

Where personal data have been received from or made available by the competent authority of another Member State, those data may be further transmitted to authorities other than competent authorities only in particular individual and well-founded cases and subject to the preconditions laid down in Article 8a, only if the Member State that transmitted or made available the data concerned has given its prior consent to their further transmission.

Amendment 37
Article 12b (new)

Article 12b

Further transmission to private parties

Where personal data have been received from or made available by the competent authority of another Member State, those data may be further transmitted to private parties only in particular cases and subject to the preconditions laid down in Article 8b, only if the Member State that transmitted or made available the data concerned has given its prior consent to their further transmission.

Amendment 38
Article 12c (new)

Article 12c

Further transmission to third countries or international bodies

Where personal data have been received from or made available by the competent authority of another Member State, those data may not be further transmitted to competent authorities of third countries or international bodies unless the
Transmission to authorities other than competent authorities

Member States shall provide that personal data received from or made available by the competent authority of another Member State are further transmitted to authorities, other than competent authorities, of a Member State only in particular cases and if all of the following requirements are met:

(a) the transmission is provided for by law clearly obliging or authorising it and

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

or

necessary because the data concerned are indispensable to the authority to which the data shall be further transmitted to enable it to fulfil its own lawful task and provided that the aim of the collection or processing to be carried out by that authority is not incompatible with the original processing, and the legal obligations of the competent authority which intends to transmit the data are not contrary to this,

or

undoubtedly in the interest of the data subject and either the data subject has consented or circumstances are such as to allow a clear presumption of such consent.

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

Article 14

Article 14

Transaction to private parties

Member States shall, without prejudice to national criminal procedural rules, provide that personal data received from or made available by the competent authority of another Member State can be further transmitted to private parties in a Member State only in particular cases and if all of the following requirements are met:

(a) the transmission is provided for by law clearly obliging or authorising it, and

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

(c) the competent authority of the Member State that has transmitted or made available the data concerned to the competent authority that intends to further transmit them has given its prior consent to their further transmission to private parties.

Amendment 40

Article 15

Article 15

Transfer to competent authorities in third countries or to international bodies

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

(a) The transfer is provided for by law clearly obliging or authorising it.

(b) The transfer is necessary for the purpose the data concerned were transmitted or made available for or for the purpose of the prevention, investigation, detection or prosecution of criminal offences or for the purpose of the prevention of threats to public security or to a person, except where such considerations are overridden by the need to protect the interests or fundamental rights of the data subject.
(c) The competent authority of another Member State that has transmitted or made available the data concerned to the competent authority that intends to further transfer them has given its prior consent to their further transfer.

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

2. Member States shall ensure that the adequacy of the level of protection afforded by a third country or international body shall be assessed in the light of all the circumstances for each transfer or category of transfers. In particular, the assessment shall result from an examination of the following elements: the type of data, the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the third country or body in question, the professional and security rules which are applicable there, as well as the existence of sufficient safeguards put in place by the recipient of the transfer.

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

4. Where, under the procedure provided for in Article 16, it is established that a third country or international body does not ensure an adequate level of protection within the meaning of paragraph 2, Member States shall take the measures necessary to prevent any transfer of personal data to the third country or international body in question.

5. In accordance with the procedure referred to in Article 16, it may be established that a third country or international body ensures an adequate level of protection within the meaning of paragraph 2, by reason of its domestic law or of the international commitments it has entered into, for the protection of the private lives and basic freedoms and rights of individuals.

6. Exceptionally, personal data received from the competent authority of another Member State may be further transferred to competent authorities of third countries or to international bodies in or by which an adequate level of data protection is not ensured if absolutely necessary in order to safeguard the essential interests of a Member State or for the prevention of imminent serious danger threatening public security or a specific person or persons.
Amendment 41

Article 16

Committee

1. Where reference is made to this Article, the Commission shall be assisted by a Committee composed of the representatives of the Member States and chaired by the representative of the Commission.

2. The Committee shall adopt its rules of procedure on a proposal made by the Chair on the basis of standard rules of procedure which have been published in the Official Journal of the European Union.

3. The representative of the Commission shall submit to the committee a draft of the measures to be taken. The Committee shall deliver its opinion on the draft within a time limit which the chairperson may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 205(2) of the Treaty establishing the European Community, in the case of decisions which the Council is required to adopt on a proposal from the Commission. The votes of the representatives of the Member States within the committee shall be weighted in the manner set out in that Article. The chairperson shall not vote.

4. The Commission shall adopt the measures envisaged if they are in accordance with the opinion of the Committee. If the measures envisaged are not in accordance with the opinion of the Committee, or if no opinion is delivered, the Commission shall, without delay, submit to the Council a proposal relating to the measures to be taken and shall inform the European Parliament thereof.

5. The Council may act by qualified majority on the proposal, within two months from the date of referral to the Council.

If within that period, the Council has indicated by qualified majority that it opposes the proposal, the Commission shall re-examine it. It may submit an amended proposal to the Council, resubmit its proposal or present a legislative proposal. If on the expiry of that period the Council has neither adopted the proposed implementing act nor indicated its opposition to the proposal for implementing measures, the proposed implementing act shall be adopted by the Commission.

Amendment 42

Article 18

Member States shall provide that the competent authority from or by whom personal data were received or made available will be informed on request about their further processing and the achieved results.

Amendment 43

Article 19, paragraph 1, point (c) indent 4a (new)

— the time limits for storing the data,
Amendment 44

Article 19, paragraph 2, introductory part and points (a) and (b)

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

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

(b) to avoid prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competent authorities,

Amendment 45

Article 19, paragraph 4

4. The reasons for a refusal or restriction according to paragraph 2 shall not be given if their communication prejudices the purpose of the refusal. In such case the controller shall inform the data subject that he may appeal to the competent supervisory authority, without prejudice to any judicial remedy and without prejudice to national criminal procedure. If the data subject lodges an appeal to the supervisory authority, the latter shall examine the appeal. The supervisory authority shall, when investigating the appeal, only inform him of whether the data have been processed correctly and, if not, whether any necessary corrections have been made.

Amendment 46

Article 20, paragraph 1, introductory part

1. Where the data have not been obtained from the data subject or have been obtained from him without his knowledge or without his awareness that data are being collected concerning him, Member States shall provide that the controller or his representative must, at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, within a reasonable time after the data are first disclosed, provide the data subject with at least the following information free of cost, except where he already has it or the provision of the information proves impossible or would involve a disproportionate effort:

Amendment 47

Article 20, paragraph 2, introductory part and point (a)

2. The information laid down in paragraph 1 shall not be provided if necessary

(a) to enable the controller to fulfil its lawful duties properly,
Amendment 48

Article 21, paragraph 1, point (c)

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

Amendment 49

Article 21, paragraph 2, introductory part and point (a)

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

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

Amendment 50

Article 22a (new)

Article 22a

Automated individual decisions

1. Member States shall grant the right to every person not to be subject to a decision or action which produces legal effects concerning him or significantly affects him and which is based solely on the automated processing of data intended to evaluate certain personal aspects relating to him, such as his reliability, conduct, etc.

2. Subject to the other Articles of this Framework Decision, Member States shall provide that a person may only be the subject of a decision or action of the kind referred to in paragraph 1 if that decision or action is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests, such as readily available means allowing him to be informed about the logic involved in the automated processing of data concerning him and to put his point of view, unless this is incompatible with the purpose for which data are processed.

Amendment 51

Article 24, paragraph 1, subparagraph 2

Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected. Measures shall be deemed necessary where the effort they involve is not disproportionate to the objective they are designed to achieve in terms of protection.
Amendment 52

Article 24, paragraph 2, subparagraph 1a (new)

Member States shall ensure that the effectiveness of the measures set out in the first subparagraph is monitored systematically and shall report regularly on their effectiveness.

Amendment 53

Article 25, paragraph 1, introductory part

1. Member States shall provide that every controller keeps a register of any processing operation or sets of such an operation intended to serve a single purpose or several related purposes. The information to be contained in the register shall include

Amendment 54

Article 26, paragraph 3

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

Amendment 55

Article 29, paragraph 2

2. Member States shall provide for effective, proportionate and dissuasive criminal sanctions for intentionally committed offences implying serious infringements of provisions adopted pursuant to this Framework Decision, notably provisions aimed at ensuring confidentiality and security of processing.

Amendment 56

Article 29, paragraph 2a (new)

2a. The Member States shall ensure that offences committed by private parties collecting or processing personal data in connection with public administration which constitute serious violations of the provisions adopted pursuant to this Framework Decision, particularly of its provisions on confidentiality and the security of data processing, render the offender liable to effective, proportionate and dissuasive penalties under the criminal law.

Amendment 57

Article 30, paragraph 4, subparagraph 1a (new)

In particular, each supervisory authority shall, at the request of a data subject, examine the lawfulness of the processing of personal data relating to that person. It shall inform the data subject of the outcome of its examination.
Amendment 58
Article 31, paragraph 2, subparagraph 1

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

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

Amendment 59
Article 31, paragraph 2, subparagraph 2a (new)

The chairperson of the Working Party set up by Article 29 of Directive 95/46/EC shall participate or be represented in the meetings of the Working Party.

Amendment 60
Article 31, paragraph 3

3. The Working Party shall take its decisions by a simple majority of the representatives of the supervisory authorities of the Member States.

3. The Working Party shall take its decisions by a simple majority of the representatives of the supervisory authorities of the Member States and after consulting the European Data Protection Supervisor.

Amendment 61
Article 34a (new)

Article 34a

Relation to Europol, Eurojust and the Customs Information System

Not later than two years from the date referred to in Article 35(1) and pursuant to Articles 29, 30(1)(b) and 31(1)(c) of the Treaty on European Union, the Article 29 Working Party shall make recommendations to the Commission with a view to making the specific data protection provisions which are applicable to Europol, Eurojust and the Customs Information System fully consistent with this Framework Decision.

Europol, Eurojust and the Customs Information System shall retain those of their data protection rules which clearly provide that personal data may be processed, consulted or transmitted only on the basis of more specific and/or protective conditions or restrictions.