Conference of European Data Protection Authorities

Brussels, 24 January 2006

Opinion on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

Executive Summary

The Conference considers that we are on the eve of a major development for fundamental rights and freedoms, which has been preceded by preparatory work that has been developing over several years and has now been taken up by the Commission with a view to creating an area of freedom, security and justice.

The Data Protection Authorities very much welcome the proposed introduction of specific data protection principles in the third pillar to safeguard citizens.

An innovative approach such as the one envisaged in The Hague Programme on judicial and police co-operation requires corresponding innovations in terms of safeguards.

These Authorities consider that the introduction of new, systematic, well-balanced safeguards will contribute to effectively enhancing the prevention of and fight against crime.

These Authorities call for the adoption of the present draft as supplemented by their opinion with a view to achieving a comprehensive data protection framework. In this manner, a system of safeguards would be set up and applied not only to the data transmitted to and/or received from other Member States, but to the whole of processing operations concerning personal data in the law enforcement sector, including the use of non-automated data.

Consistent solutions might be devised in order to also apply the new principles to Europol, Eurojust, and the Customs Information System.

The Authorities encourage the approximation of the laws and regulations of Member States; to that end, they advocate that the final wording of these principles be based on indications as clear-cut and precise as possible in order to prevent interpretive issues and excessively divergent applications.

In this respect, the Authorities request that some provisions in the draft be clarified, supplemented or amended, and confirm their readiness to contribute further to the launch of this important instrument.

I. Introduction

A harmonised standard of data protection applicable to all law enforcement activities has been the subject of discussion for several years.

The developments in the past years in the field of law enforcement driven by the demands of tackling terrorism and serious crime, call for further investment in appropriate safeguards to guarantee a high standard of data protection, taking into account the fundamental rights enshrined in existing legal instruments.

Supporting this call, The Hague Programme promotes the development of adequate safeguards and effective legal remedies for the transfer of personal data for the purpose of police and judicial cooperation in criminal matters. The European Parliament also recommended harmonizing existing rules on the protection of personal data in the instruments of the third pillar, bringing them together in a single instrument that guarantees the same level of data protection as provided for under the first pillar.
Furthermore, the 2005 Spring Conference of the European Data Protection Authorities in Krakow adopted a Declaration and Position Paper advocating the development of a data protection legal framework applicable to law enforcement activities and providing a tailor made set of rules.[1]

On 4 October 2005, the Commission presented a proposal for a Council Framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[2]

The Conference very much welcomes this proposal that should be recognised as an important step towards the creation of harmonised and appropriate data protection safeguards. The Conference has adopted the following opinion at its Conference on 24 January 2006 in Brussels.

II. Introductory remarks

The EU is obliged to respect fundamental rights, as guaranteed by the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union.

In addition to the right to respect for private and family life guaranteed by Article 8 of the ECHR and reaffirmed by Article 7 of the Charter of Fundamental Rights, the right to data protection is enshrined in Article 8 of the Charter.

Pursuant to the fundamental rights outlined above, the 1981 Council of Europe Convention on data protection (Convention 108) sets out specific principles of data protection and is applicable in the third pillar.[3] More detailed provisions can be found in a Recommendation on the use of personal data in the police sector, which was adopted by the Council of Europe's Committee of Ministers.[4]

---

1 Krakow Declaration and Position Paper, Krakow 25-26 April 2005
2 COM(2005) 475
3 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (Convention 108)
4 Recommendation No. R (87) 15, of 17 September 1987

According to the explanatory memorandum, this Recommendation has been taken into account in order to transpose its main principles into legally binding provisions at EU level. The importance of this Recommendation justifies that reference is made to that Recommendation in the preamble of the proposed framework decision.

It should be stressed that personal data processed for law enforcement purposes are particularly delicate. Apart from the character of the data and the impact on the data subject when his data are processed by law enforcement authorities, the nature of the processing and the fact that this happens in most cases without the knowledge of the person concerned, forces the introduction of a high level of protection. It should also be stressed that any use of these data may have serious and sometimes irreversible consequences.

The present proposal provides for a good instrument to enhance the safeguards of the data subject and at the same time will introduce a platform for harmonized processing of law enforcement data.

III. General remarks

In the Krakow Declaration the Conference stated that *"In order to avoid a divergence between the First and the Third Pillars which would have a negative impact on enforcement and transparency and in view of the Charter of Fundamental Rights and the forthcoming Constitution for Europe which will abolish the Pillars, the Conference calls to preserve - and where necessary to regain - the coherence, the consistency and the unity of data protection. The principles of Directive 95/46 should form the common core of a comprehensive European data protection law."*

The Conference welcomes the approach to follow existing and proven principles and definitions, notably those laid down in Directive 95/46/EC. This is undoubtedly in the interests of guaranteeing consistency in data protection in the EU and shall at the same time provide for specific rules in the area of law enforcement. The specific task of law enforcement authorities, the different developments in this area and the character of personal data involved make it necessary to develop common standards and to set up effective safeguards.

The Conference considers that we are on the eve of a major development for fundamental rights and freedoms, which has been preceded by preparatory work that has been developing over several years and has now been taken up by the Commission with a view to creating an area of freedom, security and justice.

The Data Protection Authorities welcome the proposal introducing principles to safeguard citizens. An innovative approach such as the one envisaged in The Hague Programme on judicial and police co-operation requires corresponding innovations in terms of safeguards. These Authorities consider that the introduction of new, systematic, well-balanced safeguards will contribute to effectively enhancing the prevention of and fight against crime. These Authorities call for the adoption of the present draft as supplemented by their opinion with a view to achieving a comprehensive data protection framework. In this manner, a system of safeguards would be set up and applied not only to the data transmitted to and/or received from other Member States, but to the whole of processing operations concerning personal data in the law enforcement sector, including the use of non-automated data. Consistent solutions might be devised in order to also apply the new principles to Europol, Eurojust, and the Customs Information System. The Authorities encourage the approximation of the laws and regulations of Member States; to that end, they advocate that the final wording of the new principles be based on indications as clear-cut and precise as possible in order to prevent interpretive issues and excessively divergent applications. In this respect, the Authorities request that some provisions in the draft be clarified, supplemented or amended, and confirm their readiness to contribute further to the launch of this important instrument.

Recalling its Krakow Declaration and Position Paper, the Conference welcomes that the object of the present proposal sets common standards for all processing of personal data in the field of law enforcement. Developments to improve the fight against crime go beyond the simple exchange of personal data and justify the approximation of Member States' laws. The fundamental rights of the individual are at stake and need adequate and harmonized data protection safeguards that should not be limited to exchanged data.

The proposed framework decision uses the term "public security" in the Articles 11-15. The Conference notes that this term has a different meaning in the national laws of some of the Member States
In view of the need to harmonize the conditions for further use of personal data as regulated in Article 11-15, it is suggested to avoid using terms which may have different connotations.

IV. Specific remarks

The Conference has some specific remarks concerning the followings subjects.

Preamble

In preamble (9) “the (…) European citizens” should be replaced by "everyone" . Data protection is a right of every human being.

Preamble 25 as well as Article 34(2), state that any reference to the Council of Europe Convention of 28 January 1981 (Convention 108) should be read as a reference to this framework decision. However, it is not explained in which instruments and why this should be the case. It also appears to be inconsistent with Article 3(2) as both the Europol Convention and Eurojust Decision refer specifically to the Convention 108.

The use of biometric data and DNA profiles in law enforcement activities is increasing. The character of these data justifies the introduction of a preamble calling for special attention to these data.

Chapter I, object, definitions and scope

Article 1
Article 34(2)(b) of the Treaty on the European Union is used as legal basis for the proposal. The Council thus clearly underlines its aim to approximate laws and regulations of Member States. This is reaffirmed in Article 1(1), stating that the object of the proposed framework decision is to set common standards to ensure protection of individuals with regard to the processing of personal data in law enforcement. Against this background, Article 1(2) only makes sense if the proposed framework decision results in a complete harmonization of data protection law concerning the police and judicial cooperation in the EU.

Article 2

Law enforcement authorities use various techniques to collect and further process personal data. This includes the processing of different formats of information relating to natural persons such as sound and images. In order to be consistent with the Directive 95/46/EC, the proposed framework decision should also apply to these data. The Conference suggests introducing an explanation in the preamble that the definition of personal data also includes these different formats.

Article 3

According to preambles 21 and 22, the proposed framework decision will *replace* the data protection regime of the Schengen Acquis, including the rules applicable to the Schengen Information System, as well as those that will be applicable to SIS II.

It should be recognised that the Schengen Information System contains a separate and specific form of processing of personal data. At present, the Schengen Acquis provides for "tailor made' data protection rules. The replacement of these tailor made rules by more general rules provided for by the proposed framework decision should not lead to a lower level of protection.
For further detailed comments on this topic, the Conference refers to the opinions of the Schengen Joint Supervisory Authority, the European Data Protection Supervisor (EDPS) and the Article 29 Working Party on the proposed legal basis for SIS II.

The Conference stresses the need to regulate the processing of all manual data. In the field of law enforcement activities, data conservation in paper records still plays an important role. Therefore the same level of data protection should apply for all manual data processing as for structured files.

Article 3 furthermore excludes Europol, Eurojust and the Customs Information System from the application of the proposed framework decision. The Conference recognizes that there are strong reasons for Article 3(2) as a short term-measure. However, the aim should be for these organisations to come within the scope of the proposed framework decision even if they then need to retain some additional specific rules to reflect their particular circumstances.

Chapter II, general rules of the lawfulness of processing of personal data

The application of the proposed framework decision to all data processing by law enforcement authorities means that the general rules of the lawfulness should apply to all aspects of processing. These general rules should thus also provide for the rules of further processing of data irrespective of whether those data were transmitted by another Member State. In view of this, the rules in Chapter III should be included in Chapter II, except for those provisions that provide for additional safeguards relating to transmitted data.

Article 4

The principles in paragraph 1 concerning the quality of data are consistent with the Directive 95/46/EC. Article 4(1)(d) introduces a provision according to which Member States may provide for the processing of data to varying degrees of accuracy and reliability. The Conference understands that the specific character of law enforcement justifies this difference. However, in view of the importance and impact of the use of such data, more detailed regulations for their distinction to varying degrees of accuracy and reliability should be developed, strictly implemented and controlled.

Connected with this subject is the third paragraph of Article 4, calling for a “clear distinction to be made between personal data” of the categories of persons mentioned in that paragraph.
The Conference understands that Article 4(3) provides for an extra safeguard, distinguishing categories of persons, based on the reason for processing their data. However, the proposed framework decision gives no further indication of the purpose for making that distinction.
Such a distinction could for example be used to create limitations in the further use of these data, limitations based on the category of person and/or the kind of data processed. It should be clear that data considered as not reliable may not always be used for all law enforcement purposes. The same applies for the categories of persons. Data concerning non-suspects, collected and used for a specific investigation, may not be used for any other law enforcement activity.

The Conference advocates the introduction of a system limiting the further use of personal data pursuant to Articles 11-15 of the proposed framework decision. The limitations should also be based on the categories of persons and the classification of data.

Chapter II does not contain specific rules on the further processing of exchanged data by the recipient that has been collected using special investigation methods, especially covert or mandatory collection of personal data without the knowledge of the citizen concerned.
For example, data collected by interference with the secrecy of telecommunications ought to be classified as such and the recipient ought to be obliged to respect special limitations for further use in compliance with the classification of the Member State where they have been collected.

The Conference advocates a new paragraph in Article 4 introducing an obligation for the recipient to act in conformity with any limitation of use to which the controller of the data is subject.

The Conference further wonders what is meant with the sentence in the last indent of Article 4(3).
The processing of data on persons who are not suspected of having committed any crime (other than victims and witnesses) should only be allowed under certain specific conditions and when absolutely necessary for a legitimate, well-defined and specific purpose.
The processing of data on non-suspects, such as when making speculative enquiries or for the purpose of establishing whether or not a suspicion relating to a serious criminal activity might be justified, should be restricted to a limited period, and the further use of these data for other purposes should be prohibited.

Paragraph 4, first indent, contains a specification of the term “necessary” in the context of processing data for the purposes of the present draft. The Conference notes that this specification is too wide and in contradiction with the restrictive notion of the word "necessary". Paragraph 4 for example includes terms such as "making possible" and "facilitating or accelerating" which in fact indicate unlimited processing of personal data.
The Conference strongly suggests redrafting this text, taking into account existing case law of the European Court of Human Rights relating to Article 8 ECHR.
Since this subject is closely related to the criteria for making data processing legitimate, the Conference further suggests moving this paragraph to Article 5.

Article 6

Article 6 (2) provides for more opportunities to process sensitive data in comparison with Principle 2.4 of the Council of Europe Recommendation No. (87) 15. That principle allows processing of sensitive data for police purposes only if absolutely necessary for the purposes of a particular inquiry. In view of the sensitive character of the data and the implications of their use, it is necessary to limit the processing to a particular inquiry.
Furthermore, it is suggested to introduce an obligation to the Member States to implement special organizational requirements for the processing of sensitive data.

Article 7

Article 7, dealing with the time limits for the storage of personal data, does not provide for absolute time limits. Article 7 follows the general principle laid down in Article 4(1)(e): personal data shall be stored for no longer than necessary for the purpose for which it was collected.
However, Article 7 also creates the possibility to introduce other time limits by national law. This opportunity is not acceptable for different reasons. Limited storage is a basic principle of data protection and derives from the fundamental right of respect for private life. It should not be overridden simply because a Member States chooses to legislate otherwise. This article introduces a very general exception which might influence the harmonisation effect of the proposed framework decision. Different time limits in different Member States for the same data will also have a negative effect on the exchange of data. On several occasions law enforcement authorities referred to the different storage periods as a reason for not exchanging information.
The Conference proposes to delete this exception.

Chapter III, Specific forms of processing

The Conference refers to its comment on Chapter II that those provisions of Chapter III that will be generally applicable to the processing of personal data should be included in Chapter II.

SECTION I- transmission of and making available personal data to the competent authorities of other Member States

Article 8

In order to maintain consistency with the general principles in Chapter II, it should be made clear that Article 8 refers to the personal data "collected and processed in accordance with Article 5 of the proposal".
The communication of such personal data must respect principle 5 of Recommendation 87/15 of the Council of Europe, which specifically addresses all the tasks police authorities are entrusted with for the prevention and suppression of criminal offences and the maintenance of public order (reference is made to the definition of "for police purposes" contained therein).
In particular, Principle 5.1 "Communication within the police sector" underlines the need to demonstrate the existence of "a legitimate interest for such communication within the framework of the legal powers of these bodies".
As the evaluation of the Recommendation has shown, its principles are of great importance for the lawful processing of personal data in the field of the judicial and police activities aimed at prevention as well as the performance of police tasks – including public prosecutors' activities in this field - so as to ensure respect for fundamental human rights and in particular for Article 8 of the ECHR.

The Conference proposes to amend the text as follows.

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.*

Article 9

The Conference suggests to add in Article 9(1) a reference to Article 4 (principles relating to data quality) in order to stress, as also highlighted by the EDPS in his opinion (point 52), that the provisions of Chapter III should offer additional protection to data subjects and prevent the risk of lowering such protection.
Consequently the words "Furthermore…inaccurate" in Article 9(5) should be deleted.

Article 9(7) sums up three reasons for deletion of data received from another Member State. There is a close relation between this paragraph and Article 4 (1)(c). In view of this, the Conference suggests to underline the existing connection between the first two reasons for deletion of received data and the third one, by introducing at the end of the second indent "….**and, in any case** if these data .."-.

Article 10

Like the EDPS (point 133 of the EDPS' opinion), the Conference believes that "an effective monitoring of a proper processing of personal data must focus not only on the lawfulness of the transmission of personal data between authorities, but also on the lawfulness of the access by those authorities. It is therefore necessary to log or document "access" to data." The Conference suggests amending the first two paragraphs accordingly.

In view of the tasks of the supervisory authorities, Article 10(3) should specify that logs should be "**kept at the disposal of the competent supervisory authority and** communicated without delay **to the said** authority on request."

Article 10 does not deal with a time limit for the storage of log data. It would be appropriate to set a certain minimum time limit for the storage in the proposed framework decision.

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

Article 11

Article 11(1) defines the purposes of the further processing of personal data. Referring to its comments concerning the scope of the proposed framework decision, the Conference advocates that Article 11 should apply to all data processing, and should not be limited to exchanged data. Article 11 should furthermore correspond with the principles governing the collection of the data, i.e. Article 4 (1)(b) and Article 5. It should be noted that Article 5 defines the criteria for making the processing of personal data legitimate, and requires that "the processing [be] 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". However Article 11(1)(b) includes

other reasons legitimating the further processing of data such as preventing threats to public security or to a person.

The Conference notes that the further use of personal data should in principle be limited to the initial purpose of the processing. However, the Conference is well aware of the need to use data for other purposes. The provisions concerning the further use should therefore allow some flexibility Recalling its Krakow position paper, personal data should only be collected and processed for legitimate, well-defined and specific law enforcement purposes. Such exceptions could apply when absolutely necessary, in a specific case, for the prevention, investigation, detection and prosecution of criminal offences or for the protection of interests or fundamental rights of a person, taking into account any special limitations relating to the category of personal data.
The Conference was concerned as to how in practice the concept of prior consent would work and whether it is realistic to include it in this article without any limitation. The Conference also considered that the use of the term "consent" should be confined to the position of the data subject. In the context of law enforcement authorities, the term "authorisation" or "approval" is more appropriate.

Articles 12-15

In the position paper adopted at the Krakow Conference, general rules for the further processing of personal data are defined. These rules should be used as a basis for the assessment of Article 12-15.

Basic rule is the relation between the further processing and transmission of data with the purpose of the collection and processing. This requires strict respect of the general principles contained in Chapter II.

It should be furthermore be stressed that the recipients as referred to in Article 13 and 14 may only use the data in accordance with the relevant national data protection rules.

Article 13

Article 13 allows the transmission to authorities other than competent authorities without sufficient limitations. The Conference refers to the more limited possibilities mentioned in Principle 8 of the Position Paper adopted in Krakow. Further transmission and use of personal data collected and processed for law enforcement purposes must only be allowed under specific, well-documented circumstances that must be provided for by law and necessary in an individual case.

Article 14

The current wording of Article 14 seems to better reflect the necessary requirements. It should be clarified in the text that the words “only in particular cases” refer to a specific individual.

Article 15

In view of consistency, Article 15 should apply to all personal data processed irrespective of their origin. Only Article 15(1)(c) provides for additional rules for exchanged data.
Article 15(6) provides for an exception to the basic rules of Article 15 in case where essential interests of a Member State or the prevention of imminent serious danger threatening public security or a specific person or persons justify such exception. In line with the obligation of Article 15(1)(c), the Conference suggests introducing, in cases where the data have been received from another member State, an obligation to inform the competent authority of that Member State of the use of this exception.

Chapter IV, Rights of the Data subject

The processing of personal data in the third pillar requires a high level of protection because of the sensitivity of the data and the serious and harmful consequences this may have for the data subject, especially in relation to the fear of new terrorist attacks.

The Conference welcomes the provisions related to the data subject rights which are consistent with the general rules of data protection legislation. Moreover, these provisions provide for a harmonized set of rules while the current situation varies a lot from one Member State to another. Indeed, in some Member States the data subject has a direct right of access to his/her data, while in other Member States this right is only indirect. Information communicated to the data subject when he/she exercises his/her right of access (direct or indirect) is different from one Member State to another, some providing a lot of information while others do not communicate any information at all.

Like the EDPS, the Conference regrets that the proposal does not address the important issue of automated individual decisions. This is especially important in the third pillar where consequences of the processing of personal data may seriously and harmfully affect the data subject. Indeed, these data are mainly processed by authorities having public coercive powers. Moreover, the data processed are often only based on suspicions. Finally, it must be kept in mind that personal data will be exchanged on a very large scale increasing the risk of errors.

Therefore, the Conference also recommends introducing a specific provision in the proposal on automated individual decisions. Such a decision should only be authorized by a law which lays down measures to safeguard the data subject's legitimate interests. Moreover, arrangements should be made in order to allow the data subject to put across his/her point of view and to know the logic of the decision.

Article 19

Article 19(2) provides for a list of derogations from the obligation of the data controller to inform the data subject about several elements.

The Conference is aware that it can be necessary for law enforcement purposes not to inform the data subject that his/her data are processed. However, since this is a derogation of a fundamental right, it has to be analyzed according to the principle of proportionality. In other words, the derogation must be strictly defined and applied on a case-by-case basis referring to a specific individual.

One of the derogations is to enable the controller to fulfil its lawful duties properly (letter a). This derogation is so broad that it could become the rule. Moreover, it overlaps the derogation provided under letter b, according to which the provision of information shall be refused or restricted if necessary "*to avoid prejudicing of ongoing investigations, inquiries or proceedings or the fulfilment of the lawful duties of the competent authorities*". As this derogation seems justified and protects police and judicial work, the former one is clearly too broad and should be deleted.

The Conference wonders why a distinction is made between the duties of the "controller" (letter a) and the duties of the "competent authorities" (letter b). Does it mean the controller benefits from a broader derogation when the data are processed for its own duties than when they are processed by

competent authorities? The derogation is much too broad and should be deleted. The obligation to inform the data subject should only be limited for both of them (controller and competent authorities) if it may prejudice the fulfilment of their lawful duties. Letter b could be completed as follows: "(…) **or the fulfilment of the lawful duties of the controller and/or the competent authorities"**.

The Conference welcomes the last indent which reiterates the obligation to always strike the balance between the rights of the data subject and the interests of the controller.

Articles 19(3) and 19(4) refer to the refusal or restriction to give information to the data subject. This might cause some confusion with the right of access. Indeed, the data subject does not have to request the information (contrary to the rights of access), the information must be automatically given to him/her. These paragraphs should be redrafted taking into account these differences.

Article 20

Article 20(1) stipulates that the controller has to either inform the data subject at the time of undertaking the recording of personal data or, if disclosure is envisaged, within a reasonable time after the data are first disclosed. The logic here is unclear. Data subjects are likely to be more concerned about the possible disclosure of their data than about mere recording. However, it is where disclosure is envisaged that the provision of information to the data subject can be delayed even beyond the point at which the data are disclosed. When disclosure is not envisaged, the provision of information has to be immediate. The Conference proposes that Article 20(1) should be amended to provide that information should be given to the data subject within a reasonable time after undertaking the recording of personal data and, in any case, no later than before the data are first disclosed. The Conference considers that this would simplify the article, be of greater benefit to data subjects and be less burdensome for data controllers.

Article 21

Article 21 guarantees data subjects rights to be obtained from the controller. It is important to defines these specific rights, but the Conference suggests to leave it up to national law to determine the appropriate means of exercising these rights. Article 21(1) and the specific provisions in paragraphs 3 and 4 should be redrafted in that sense.

According to Article 21(1)(c), the data subject has the right to obtain from the controller "*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*".
The Conference wonders why reference is made to impossible or disproportionate effort to exempt the controller to notify third parties of any rectification, erasure or blocking of data.

It should be noted that Article 10 requires the Member State to log/document the transmission and reception of data. Furthermore, Article 22 states that appropriate technical measures have to be taken to ensure that, in cases where the controller rectifies, blocks or erases personal data following a request, a list of the suppliers and addressees of these data is automatically produced. Moreover, the controller shall ensure that those included in the list are informed of the changes performed on the personal data. In view of these two provisions, the Conference wonders why it still could be impossible or difficult for the controller to notify third parties of any change related to the data disclosed. Therefore, the sentence "*unless this proves impossible or involves a disproportionate effort*" should be deleted.

Since Chapter IV does not contain special provisions concerning data from another Member State, and in view of the aim to harmonize data protection rules, the right to rectify or erase data should apply to all data processed in a Member State irrespective of their origin. It is then important to ensure Member States undertake mutually to enforce final decisions taken by courts or authorities as referred to in Article 30.

In relation to Article 21(2) the Conference refers to the remarks made on Article 19(2).

Chapter V, Confidentiality and security of processing

Chapter V of the proposed framework decision deals with confidentiality (art 23) and security (art 24) of processing, including register (art 25) and prior checking (26).
The provisions are generally consistent with current EU data protection legislation from Directive 95/46/EC, which reveals a positive approach. Nevertheless, it contains some provisions which do not take into account the specific and sometimes very sensitive aspects of the processing of personal data by police and judicial authorities in the third pillar which ought to demand a higher level of protection.

Article 23

Article 23, second sentence, contains a provision under which "all persons called upon to work with or within a competent authority of a Member State shall be bound by strict confidentiality rules". The Conference supports this provision, and calls for the introduction of more specific indications as to the type of confidentiality rules they will have to refer to. The Conference furthermore suggests that this provision should be based on effective legal provisions.
In order to create a coherent security framework, the security measures listed in Article 24(2) should also include an obligation to provide for measures dealing with confidentiality at the national level unless "a common level of confidentiality" is defined.

Article 24

The Conference has some concerns about the meaning of the last sentence in Article 24 (1), which induces a proportionate relationship between "necessary measures" and "the required effort involved to have them put in place". The recommended measures will thus be weakened by such a restrictive condition. The Conference suggests deleting the last sentence.

The Conference notes with satisfaction the number of security measures provided for in Article 24(3). It is suggested to add some provisions at point g making it possible to carry out some control over the objective itself of the data processing system.

Article 25

The register provided for in Article 25 is similar as the provisions on notification referred to in Article 19(1) of the Directive 95/46/CE. However, the Conference notes that the proposed framework decision does not include any obligation of notification. The Conference suggests that notification should be made compulsory, as it is provided for in the Directive 95/46/CE in Article 18 and 19, including provisions referring to the content of notification, appropriate exceptions, and the possible appointment of a data protection officer pursuant to national data protection legislation (as in Article 19(2) of Directive 95/46/EC).

The conditions and procedures of notification to the supervisory authority should furthermore refer to the national legislations in the field of data protection. In view of this it is suggested to replace in Article 25(2) the reference to Members States by the following wording: **"The conditions and procedures under which information referred to in paragraph 1 must be notified to the supervisory authority will be specified by national data protection legislation".**

Article 26

Article 26(3) contains a provision for carrying out "prior checking 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".

Considering Article 5, requiring a law to legitimate data processing by law enforcement authorities, and the logical and legitimate intervention of data protection authorities in the legislative process in such a sensitive field dealing with the processing of personal data, the Conference recommends that 26(3) should read as follows: **"Supervisory authorities shall be consulted on the provisions relating to the protection of individuals' rights and freedom when drawing up legislative measures in relation to data processing".** The Conference also suggests that such a provision should be made coherent with the provisions of Article 30(2) and Article 5.

Chapter VII, Supervisory authority and working party on the protection of individuals with regard to the processing of personal data

Chapter VII deals with the role of the supervisory authorities and of the new Working Party on the protection of individuals with regard to the processing of personal data.

The Conference welcomes the general approach in Chapter VII which has been formulated according to the model of Chapter VI in Directive 95/46/EC. This will facilitate the co-operation of the working parties competent for data protection in the first and third pillar.

Article 30

The provisions of Article 30 dealing with the supervisory authorities and their tasks are similar to those in Art. 28 (4) of the Directive 95/46/EC. However their tasks in relation to the data subject are not identical. Therefore it is suggested to add the following phrases to Paragraph 4.

„Each supervisory authority shall, in particular, hear claims for checks of the lawfulness of data processing lodged by any person. The person shall at any rate be informed that a check has taken place."

It seems appropriate to re-consider the wording of Paragraph 9 as it deals with a possible collision between the powers of supervisory authorities and the independence of the judiciary, whereas this should not be a cause for concern. It is up to national lawmakers, having set out the principle whereby data protection authorities should be enabled to effectively supervise lawfulness of the processing also in the judicial sector, to lay down, based on the respective experience and legal systems, any specific mechanisms and procedures that take account of the special institutional role played by the judiciary.

Article 31

Paragraph 1 describes the establishment of the working party. It seems that the wording of this paragraph is too limited. Since the objective of the proposed framework decision aims to create a full harmonisation of data protection rules in third pillar, both at national and EU level, this aim should also be reflected in the wording of this paragraph.

The creation of an autonomous body, based on the model used for the Art. 29 Working Party would provide a satisfactory solution for dealing with third pillar questions. In order to maintain a consistent approach in data protection matters, the Conference stresses the need to co-ordinate the work of these two advisory bodies. This can be achieved by stimulating a similar or equal representation in both bodies.

In order to ensure the respect of national legislation on this matter, Article 31 (2), second indent, should be completed as follows.
„The Working Party shall be composed of a representative of the supervisory authority or authorities which he represents, **in accordance with the existing national rules regulating the representation.“**

The Conference underlines the need to guarantee the independent role of the working party. The exchange of information between Member States calls for cooperation between national data protection supervisory authorities and the EDPS. This cooperation may relate to general matters but could also involve joint inspections or other supervisory tasks. This calls for a forum for these independent supervisory authorities in which it and its secretariat can operate autonomously an independently.

V Conclusion

To provide for all the necessary guarantees for an adequate level of data protection in conformity with the existing legal framework, the Conference recommends that the proposed framework decision should be amended, taking into account the remarks made in this opinion.

The EU Data protection Authorities are, of course, willing to contribute further to the development of this Council Framework Decision.