EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision concerning access for consultation of 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 (COM (2005) 600 final)

(2006/C 97/03)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to 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,

Having regard to 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, and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 29 November 2005 from the Commission;

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION

1.1. Preliminary remark

The Proposal for a Council Decision concerning access for consultation of 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 (hereinafter: 'the proposal') was sent by the Commission to the European Data Protection Supervisor (EDPS) by letter of 24 November 2005. The EDPS understands this letter as a request to advise Community institutions and bodies, as foreseen in Article 28(2) of Regulation (EC) No 45/2001. According to the EDPS, the present opinion should be mentioned in the preamble of the Decision.

The EDPS deems it important to deliver an opinion on this sensitive subject because this proposal follows directly from the establishment of the VIS, which will be subject to his supervision, and on which he has issued an opinion on 23 March 2005 [1]. In that opinion, the hypothesis of access by law enforcement authorities was already envisaged (see below); the creation of new access rights to the VIS has a determinant impact on the system, in terms of data protection. Therefore, giving an opinion on the present proposal is a necessary follow-up of the first opinion.

1.2. Importance of the proposal

a) *Context*

The present proposal is not only important on its own merits, but also because it comes within the general trend to grant law enforcement authorities access to several large scale information and identification systems. This is mentioned amongst others in the Commission's Communication of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs [2], especially in its point 4.6: '*In relation to the objective of combating terrorism and crime, the Council now identifies the absence of access by internal security authorities to VIS data as a shortcoming. The same could also be said for SIS II immigration and EURODAC data*'.

Therefore, the present proposal could be seen as a precursor of similar legal instruments developed in the context of other databases, and it is crucial to define from the beginning the cases where this access could be admissible.

---

[1] Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay-visas (COM(2004)835 final).

[2] COM (2005) 597 final

b) *Impact of a new access to the VIS*

The EDPS certainly recognises the need for law enforcement authorities to benefit from the best possible tools to identify the perpetrators of terrorist acts or other serious crime. He is also aware that VIS data may constitute, in certain circumstances, an essential source of information for these authorities.

Nevertheless, granting access to first pillar databases to law enforcement agencies, however justified it may be by the fight against terrorism, is far from insignificant. One must bear in mind that the VIS is an information system developed in view of the application of the European visa policy and not as a law enforcement tool. Routine access would indeed represent a serious violation of the principle of purpose limitation. It would entail a disproportionate intrusion in the privacy of travellers who agreed to their data being processed in order to obtain a visa, and expect their data to be collected, consulted and transmitted, only for that purpose.

Since information systems are built for a specific purpose, with safeguards, security, conditions for access determined by this purpose, granting systematic access for a purpose different from the original one would not only infringe the principle of purpose limitation, but could also make the above mentioned elements inadequate or insufficient.

In the same line of thinking, such a significant change of the system could invalidate the results of the impact assessment study (which addressed the use of the system for the original purpose only). The same is true for the opinions of the data protection authorities. It could be argued that the new proposal changes the premises of the compliance analysis made by them.

c) *Strict limitation of this access*

In the light of the comments made here above, the EDPS would like to stress that access to the VIS by law enforcement can only be granted in specific circumstances, on a case by case basis, and must be accompanied by strict safeguards. In other words, consultation by law enforcement agencies must be limited by adequate technical and legal means to specific cases.

The EDPS had already underlined this in his opinion on the VIS: '*The EDPS is aware that the law enforcement agencies are interested in being granted access to the VIS; Council Conclusions in this sense have been adopted on 7 March 2005. As the purpose of the VIS is the improvement of the common visa policy, it should be noted that routine access by law enforcement authorities would not be in accordance with this purpose. While, according to Article 13 of Directive 95/46/EC, such an access could be granted on an ad hoc basis, in specific circumstances and subject to the appropriate safeguards, a systematic access cannot be allowed*'.

In conclusion, the essential requirements could be summarized as follows:

— Systematic access should not be granted: the Decision must ensure that there is a case by case examination of the necessity and proportionality of access by third pillar authorities at all time. In this regard, a precise wording of the legal instrument is paramount, in order not to leave room for an extensive interpretation, which in turn would lead to routine access.

— In cases where access is granted, appropriate safeguards and conditions, including a comprehensive data protection regime for national use of the data, must be adopted considering the sensitive nature of this access.

1.3 **Initial comments**

The EDPS recognises that considerable attention has been devoted to data protection in this proposed instrument, mainly in limiting access to specific cases, and only in the framework of the fight against serious crime ([1]).

Among the other positive elements, the EDPS would also like to mention specifically:

— the limitation to certain forms of crime as referred to in the Europol Convention;

— the obligation for Member States to draw up a list of authorities having access and to make these lists public;

— the existence of a central access point per Member State (and of a specialised unit within Europol), allowing a better filtering of the requests for access, as well as better supervision;

— the strict rules on further transmission of data, under Article 8(5) of the proposal;

— the obligation for Member States and Europol to keep records of the persons responsible for consulting the data.

2. **ANALYSIS OF THE PROPOSAL**

2.1. **Preliminary remark**

In order to grant access to authorities on a third pillar basis, the principal first pillar VIS proposal should provide for a bridging clause, which would essentially determine the possible content of a third pillar legal instrument such as this proposal. At the time when the EDPS issued his opinion on the VIS, this bridging clause was not yet introduced, and the EDPS was not in a position to comment on it. Therefore, all comments made hereunder are made with due reservation as to the content of the bridging clause.

([1]) This is also consistent with the Council Conclusions of March and July 2005, requesting that access to VIS be granted to authorities in charge of internal security '*subject to strict compliance with the rules governing the protection of personal data*'.

2.2 **Purpose of the access**

In order to ensure a proper access limitation, it is important to carefully define the conditions for access to VIS. It is welcomed that, in addition to the proposed Decision itself, the Explanatory Memorandum and the Recitals (see especially Recital 7) make it very clear that the intention is to provide access only on a case by case basis.

One comment can be made on Article 5 of the proposal, in order to guide the interpretation thereof.

Article 5 restricts the scope of access by substantive conditions:

b) access for consultation must be necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences;

c) access for consultation must be necessary in a specific case (...), and

d) there must be reasonable grounds, based on factual indications, to consider that consultation of VIS data will contribute to the prevention, detection or investigation of any of the criminal offences in question.

These conditions are cumulative, the condition under b) being more a definition of scope *ratione materiae*. Practically speaking, it means that the authority seeking access must be confronted with a serious criminal offence as referred to under (b) of the proposal; there must be a specific case as referred to under (c). Additionally, the authority must be able to demonstrate that in that specific case, the consultation of VIS data will contribute to the prevention, detection or investigation of that offence, as foreseen under (d).

Even with this interpretation of Article 5, the EDPS is concerned by the flexible wording in point (d): 'contribute to' is rather broad. There are many cases where VIS data could 'contribute to' the prevention or investigation of a serious crime. In order to justify an access to VIS data in derogation of the purpose limitation principle, the EDPS takes the view that this consultation should 'substantially contribute to' the prevention, detection or investigation of the serious crime in question and suggests amending Article 5 accordingly.

Article 10 stipulates that the records should show the exact purpose of the access. The 'exact purpose' should comprise the elements which made the consultation of the VIS necessary in the sense of Article 5 sub (d). This would help ensuring that a test of necessity is applied for all consultations of the VIS, and reduce the risk of routine access.

2.3. **Search keys in the VIS database**

Article 5(2) and (3) provides for a two-step access to VIS data, with a set of data only accessible if a hit has occurred on the basis of the first set of data. This is in itself a sound approach. However, the first set of data seems very broad. In particular, the relevancy of data such as mentioned in 5(2) under (e) and (i) for the first set of data can be questioned:

— The 'purpose of the travel' seems to be a very general key to allow efficient interrogation of the system. Moreover, it entails a risk of profiling of travellers on the basis of that element.

— As to 'photographs', the possibility to query such a large database on the basis of photographs is limited; the results produced by such queries present in the current state of the technology an unacceptable rate of false matches. The consequences of an incorrect identification are very serious for the individual concerned.

Therefore, the EDPS requests that the data in Article 5(2) under (e) and (i) are considered as supplementary information accessible if the first consultation shows there are already data in the system and are moved to Article 5(3).

Alternatively, the possibility to query the database on the basis of photographs could be subject to an assessment of this technology by the advisory committee, and be implemented only when the technology will be mature and can be considered reliable enough.

2.4. **Application to Member States to which the VIS Regulation does not apply**

Access to the VIS for consultation can be exercised by authorities responsible for internal security from Member States which are not part of the VIS. These services have to perform the consultation via a participating Member State, with due respect for the conditions laid down in Article 5(1) (b) to (d) (i.e. on a case by case basis), and submit a duly motivated written request.

The EDPS would like to highlight the need to impose some conditions to the processing beyond the consultation. The rule applying to Member States participating in the VIS is that, once the data are retrieved from the VIS, they must be processed in accordance with the Framework Decision on Data Protection in the Third Pillar (see hereunder). The same condition should apply to the Member States to which the VIS Regulation does not apply, but which consult its data. The same reasoning should be applied concerning the keeping of records for future supervision. Therefore, the EDPS recommends adding in Article 6 of the proposal a paragraph to the effect that Article 8 and 10 of the Decision shall apply also to the Member States to which the VIS Regulation does not apply.

2.5. **Data protection regime**

a) *Application of the Framework Decision on Data Protection in Third Pillar*

Since access by authorities responsible for internal security represents an exception to the purpose of the VIS, it should be subject to a consistent data protection regime, ensuring a high level of protection to the data retrieved from the VIS and processed by national authorities or by Europol.

Article 8 of the Proposal lays down that the Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (hereinafter: 'the Framework Decision') shall apply to the processing of data pursuant to the proposed Decision. As far as data protection is concerned, the present proposal should thus be seen as a *lex specialis*, adding to or specifying the *lex generalis* (i.e. the Framework Decision). For example, the rules on onward transfer of data are stricter in this proposal and should be followed. The same goes for the grounds for access to the data.

b) *Scope*

The EDPS welcomes the fact that the data protection regime of the Framework Decision is applicable to all processing of personal data pursuant to the proposed Decision. It means that the level of data protection shall be equivalent, whatever authorities consult the VIS data.

As Article 2 uses a functional criterion to define these authorities ('those authorities in the Member States which are responsible for the prevention, detection or investigation of terrorist offences or of other serious criminal offences'), this definition could cover intelligence services as well as law enforcement authorities. Therefore, intelligence services who consult the VIS are in principle subject to the same obligations in terms of data protection, which is obviously a positive element.

However, since there may be some doubts about this interpretation concerning the applicability of the Framework Decision to intelligence services when they access VIS data, the EDPS suggests an alternative wording, such as:

'In cases where the Framework Decision (…) is not applicable, Member States shall provide for a level of data protection at least equivalent to the one ensured under the Framework Decision'.

c) *Supervision*

As to the wording of Article 8, it should be clarified that paragraph 1 concerns the processing of data within the territory of the Member States. Paragraphs 2 and 3 clarify their scope of application (data processing by Europol and the Commission), and it should be made explicit that paragraph 1 concerns another hypothesis.

The distribution of supervision competences following the respective activities of the different actors is a sound approach. One element is lacking however: the need for a coordinated approach in supervision. As already stated in the EDPS opinion on the VIS: 'As to the supervision of the VIS, it is also important to underline that the supervision activities of the national supervisory authorities, and of the EDPS should to a certain extent be coordinated. Indeed, there is a need for a harmonized implementation of the Regulation, and for working towards a common approach of common problems.

Article 35 [of the VIS proposal] should contain a provision to that effect, laying down that the EDPS shall convene a meeting with all the national supervisory authorities, at least once a year.'

The same applies to this specific use of the VIS system (with in this case the involvement of the Europol Joint Supervisory Body as well). The supervision should be totally consistent with the supervision of the 'first pillar VIS', since it is the same system. Moreover, coordination meetings convened by the EDPS, with all parties involved in supervision, is also the model which has been chosen in the context of the supervision of other large scale information systems, such as Eurodac.

The EDPS is aware that coordination is envisaged to some extent in the proposal, which mentions the role of the future Working Party on the Protection of Individuals with regard to the protection of Personal data established by Article 31 of the proposed Framework Decision. However, it should be reiterated that the supervision itself is not covered by the mission of that advisory body.

The EDPS suggests adding a provision laying down that the coordination meeting convened by the EDPS in the framework of the supervision of the 'first pillar VIS' shall also have competence for data processed pursuant to this proposal and, to that effect, the Europol JSB should be represented.

2.6. **Self-auditing**

Article 12 of the proposal provides for monitoring systems for the VIS. The EDPS takes the view that this monitoring should not only concern the aspects of output, cost-effectiveness and quality of services, but also compliance with legal requirements, especially in the field of data protection. Article 12 should be amended accordingly.

In order to perform this self-auditing of the lawfulness of processing, the Commission should be enabled to make use of the records kept in accordance with Article 10 of the proposal. Accordingly, Article 10 should provide that these records shall not only be stored for monitoring data protection and ensuring data security, but also for conducting regular self-auditing of the VIS. The self auditing reports will contribute to the supervisory task of the EDPS and the other supervisors who will be better able to select their priority areas for supervision.

3. CONCLUSION

In light of the foregoing, the EDPS underlines the crucial importance of granting access to authorities in charge of internal security and Europol, only on a case by case basis, and under strict safeguards. This aim is achieved by the proposal in a globally satisfactory way, although some improvements can be made, as proposed in this opinion:

— It should be a condition for access to the VIS according to Article 5 that consultation will 'substantially' contribute to the prevention, detection or investigation of a serious crime, and the records required in Article 10 should allow an evaluation of this condition in each individual case.

— Two search keys for access in the VIS mentioned in Article 5(2), namely 'purpose of travel' and 'photographs', should be reconsidered and made available as supplementary information in the case of a hit.

— The level of data protection applying beyond consultation should be equivalent, regardless of the authorities consulting the VIS data. Article 8 and 10 should also apply to Member States to which the VIS Regulation does not apply.

— A coordinated approach to supervision should be ensured, also with regard to access to the VIS as envisaged in this proposal.

— Provisions on monitoring systems should also ensure self-auditing of compliance with data protection requirements.

Done at Brussels on 20 January 2006.

Peter HUSTINX

European Data Protection Supervisor