EUROPEAN DATA PROTECTION SUPERVISOR

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)

(2005/C 181/06)

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 25 January 2005 from the Commission,

HAS ADOPTED THE FOLLOWING OPINION:

1. **INTRODUCTION**

1.1. **Preliminary remarks**

The setting up of the Visa Information System (VIS) constitutes an important part of the EU common visa policy and has been the subject of several instruments which are intertwined.

— In April 2003, a feasibility study ([1]) on the VIS commissioned by the Commission was produced.

— In September 2003, the Commission proposed an amendment ([2]) of a previous Regulation laying down a uniform format for visas. The main goal was to introduce biometric data (facial image and two fingerprints) in this new visa format. These biometric data would be stored on a microchip.

([1]) Visa Information System, final report, commissioned by the EC and conducted by Trasys, April 2003.
([2]) COM(2003)558 final with 2003/0217 (CNS) and 2003/0218 (CNS).

— In June 2004, a Council decision [1] launched the building process of the Visa Information System providing the legal basis for its inclusion in the budget of the EU. This decision proposed a central database comprising information related to the visa application, and envisaged a 'comitology' process in order to manage the technical development of the VIS.

In December 2004, the Commission adopted a proposal for a Regulation concerning the VIS and the exchange of data between Member States on short stay-visas [2] (hereinafter: 'the proposal') which is the subject of this opinion. A study for the Extended Impact Assessment [3] (hereinafter: 'EIA') is attached to the proposal.

However, as it is stated in its explanatory memorandum, further legal instruments will be needed to complement this regulation, in particular for:

— amending the Common Consular Instructions on visas for the diplomatic missions and consular posts of the Contracting Parties to the Schengen Convention (hereinafter, 'Common Consular Instructions'), related to the introduction of biometric data in the procedures;

— the development of a new mechanism for the exchange of data with Ireland and the United Kingdom;

— the exchange of data on long stay-visas.

As decided by the Justice and Home Affairs Council of 5-6 June 2003 and described in Article 1(2) of the June 2004 Council decision mentioned above, the VIS will be based on a centralised architecture comprising a database where the visa application files will be stored: the Central Visa Information System (CS-VIS), and a National Interface (NI-VIS) located in the Member States. The Member States will designate [4] a central national authority connected to the National Interface and through which their respective competent authorities will have access to the CS-VIS.

1.2. **Main elements of the proposal from the perspective of data protection**

The proposal aims at improving the administration of the common visa policy by facilitating the exchange of data between Member States with the setting up of a central database. The regulation envisages to introduce biometric data (photograph and fingerprint) during the application procedure, and to store them in the central database.

Biometric data might also be used in the visa sticker, as it has been foreseen in an amending regulation proposed by the Commission on the uniform format of visa with the introduction of photograph and fingerprint, stored in a microchip (still pending to Council decision based on the results of ongoing analysis).

The proposal describes in detail the different operations performed on data (entering, amending, deleting and consulting) and the different data to be added in the VIS depending on the situation of the application (acceptance, refusal, etc.).

The proposal provides for a retention period of five years for data concerning each application.

The proposal lists restrictively the competent authorities other than visa authorities, which will have access to the VIS and defines the access rights to be granted to them:

— the competent authorities for carrying out visa checks at external borders and within the territory of the Member State,

— the competent immigration authorities,

---

[1] 2004/512/EC, OJ L 213, 15.6.2004, p. 5.
[2] COM(2004)835 final with 2004/0287 (COD).
[3] Study for the Extended Impact Assessment of the Visa Information System, EPEC Final Report, December 2004.
[4] Article 24(2) of the proposal.

— the competent asylum authorities.

In the description of the operation of the VIS and the related responsibilities, the proposal underlines that the Commission processes the data of the VIS on behalf of the Member states. It describes the need for using the data processing records in order to ensure the security of data, and details the respective responsibilities to ensure this security level.

The proposal contains a chapter on data protection in which the roles of national authorities as well as the European Data Protection Supervisor (hereinafter: 'EDPS') are detailed.

The proposal entrusts the technical implementation of the VIS and the selection of the required technologies to a committee set up by Article 5(1) of Regulation (EC) No 2424/2001 on the development of the second generation Schengen Information System (SIS II).

An extended impact assessment of the VIS commissioned by the Commission and conducted by EPEC is annexed to the proposal. It concludes that the option of a VIS supported by the use of biometrics is the best available solution for improving the common visa policy.

2. **RELEVANT FRAMEWORK**

The proposal will have a major impact on the privacy and other fundamental rights of individuals; therefore it is subject to a check against the data protection principles. The main points of reference for our examination are the following.

— Respect for private life has been ensured in Europe since the adoption in 1950 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter: 'ECHR') by the Council of Europe. Article 8 ECHR stipulates 'the right to respect for private and family life'.

  According to Article 8(2) any interference by a public authority with the exercise of this right is only allowed, if it is 'in accordance with the law' and is 'necessary in a democratic society' for the protection of important interests. In the case law of the European Court of Human Rights, these conditions have led to additional requirements as to the quality of the legal basis for interference, the proportionality of any measure, and the need for appropriate safeguards against abuse.

  Basic principles for the protection of individuals with regard to the processing of personal data have been developed in the Convention on Data Protection, prepared by the Council of Europe and adopted in 1981.

— The right to respect for private life and the protection of personal data have been laid down more recently in Article 7 and 8 of the Charter of the Fundamental Rights of the European Union, which has been integrated in Part II of the new EU Constitution.

  According to Article 52 of the Charter, it is recognized that these rights may be subjected to limitations, provided that similar conditions are fulfilled as apply under Article 8 ECHR. These conditions have to be considered whenever a proposal for a possible interference is evaluated.

Today, in EU legislation, the basic rules on data protection are laid down in:

— 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 (OJ L 281, p. 31). This directive will be referred to as 'Directive 95/46/EC'. The Directive provides for the detailed principles against which the proposal will be checked to the extent in which it is to apply to the Member States. This is the more relevant since the proposal will apply together with the national legislation giving effect to the directive. The effectiveness of the proposed provisions and safeguards will thus depend on the effectiveness of that combination in every individual case.

— 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 (OJ L 8, p.1). This regulation will be referred to as 'Regulation 45/2001'. It provides similar principles as Directive 95/46/EC and is relevant in this context to the extent in which the proposal is to apply to the activities of the Commission, along with the provisions of the Regulation. This combination therefore also deserves some attention.

Directive 95/46/EC and Regulation 45/2001 must be read jointly with other instruments. In other words, the directive and the regulation, in so far as they deal with processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must be interpreted in the light of fundamental rights. This also follows from the case law of the European Court of Justice ([1]).

— Finally the EDPS will also include in his analysis the Opinion No 7/2004 of 11 August 2004 of the Article 29 Data Protection Working Party ([2]), 'on the inclusion of biometric elements in residence permits and visas taking into account the establishment of the European information system on visas (VIS)'. In this opinion, the Working Party expressed concerns about several elements of the proposal. The EDPS intends to verify whether and how the proposal has taken these concerns into account.

3. **ANALYSIS OF THE PROPOSAL**

3.1. **General**

The EDPS recognises that the further development of a common visa policy requires an efficient exchange of relevant data. One of the mechanisms that can ensure a smooth flow of information is the VIS. However, such a new instrument should be limited to the collection and exchange of data, as far as such a collection or exchange is necessary for the development of a common visa policy and is proportionate to this goal.

The establishment of the VIS may have positive consequences for other legitimate public interests, but this does not alter the purpose of the VIS. The limited purpose of the system plays a major role in determining the legitimate content and use of the system and therefore also in granting a right of access to the VIS (or to parts of its data) to authorities of the Member States, for legitimate public interests.

Moreover, the proposal introduces the use of biometrics in the VIS. The EDPS recognises the advantages of the use of biometrics, but stresses the major impact of the use of such data and suggests the insertion of stringent safeguards for the use of biometric data.

This opinion has to be read in the light of these main considerations. It is noted that the present opinion should be mentioned in the preamble of the Regulation before the recitals ('Having regard to the opinion …').

([1]) It is useful in this context to refer to the judgment of the Court of Justice in Österreichischer Rundfunk and Others (Joined Cases C-465/00, C-138/01 and C-139/01, Judgment of 20 May 2003, Full Court, (2003) ECR I-4989). The Court dealt with an Austrian law providing for the transfer of salary details on public sector employees to the Austrian Court of Auditors and their subsequent publication. In its judgment the Court lays down a number of criteria drawn from Article 8 of the European Convention on Human Rights, which should be used when applying Directive 95/46/EC in so far as this directive allows for certain restrictions to the right to privacy.

([2]) This is an independent advisory group, composed of representatives of the data protection authorities of the Member States, the EDPS and the Commission, which was set up by Directive 95/46/EC.

3.2. **Purpose**

The purpose of the VIS is of crucial importance, both in the light of Article 8 ECHR and of the general data protection framework. According to Article 6 of Directive 95/46/EC, personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'. Only a clear definition of purposes will allow a correct assessment of the proportionality and adequacy of the processing of personal data, which is critical because of the nature of the data (including biometrics) and the scale of the envisaged processing operation.

The purpose of the VIS is clearly stated in Article 1(2) of the proposal:

> 'The VIS shall improve the administration of the common visa policy, consular cooperation and consultation between central consular authorities by facilitating the exchange of data between Member States on applications and on the decisions thereto'.

Therefore all the elements of the VIS must be necessary and proportional instruments to reach this policy goal in the interest of the common visa policy.

Article 1(2) of the proposal also lists additional benefits of the improvement of the visa policy such as:

(a) preventing threats to internal security,

(b) facilitating the fight against fraud,

(c) facilitate checks at external border checkpoints.

The EDPS considers these elements as examples of positive consequences of the setting up of the VIS and of the improvement of the common visa policy, but not as autonomous purposes in themselves.

This brings two main consequences at this stage:

— 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.

  More generally speaking, an assessment on proportionality and necessity is crucial if decisions are taken in the future on whether to allow certain other authorities access to the VIS. The tasks for which access is granted must be consistent with the purposes of the VIS.

— The explicit mention of the 'prevention of threats to internal security of any of the Member States' in (a) is unfortunate. The main benefits of the VIS will be the prevention of fraud and visa shopping (the fight against fraud is also the main reason for the inclusion of biometrics in the system) ([1]). The prevention of threats to security should therefore be seen as a 'secondary' although very welcome benefit.

  The EDPS recommends that this distinction between 'purpose' and 'benefits' is made more explicit in the text of Article 1(2), for instance as follows:

  'The VIS has the purpose to improve the administration of the common visa policy, consular cooperation and consultation between central consular authorities by facilitating the exchange of data between Member States on applications and on the decisions thereto. In doing so it shall also contribute …'

([1]) The EIA states this very clearly (p.6, §2.7).: *'the inefficiencies in combating visa shopping, fraud, and in conducting checks are causing also inefficiencies in relation to internal security of the Member States'*. This implies that the threats to security are due partly to inefficient visa policy. The first thing to do in this regard is to improve the visa policy, mostly by combating fraud and perform better checks. The improvement in security will result from improvement in the visa policy.

It is also worth noting in this regard, that the 'Guidelines for the introduction of a common system for an exchange of visa data' adopted by the JHA Council on 13 June 2002 [1] placed the prevention of threats to internal security at the end of the list. It would also be possible and much more consistent with the purpose of the VIS.

3.3. **Data quality**

According to Article 6 of Directive 95/46/EC, personal data must also be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. This relates to the proportionality of the VIS in itself, but also to the data that are to be collected and stored in the VIS and to their further use, as well as to the additional safeguards applying in that context. These elements are equally essential for the evaluation of the proposal in the light of Article 8 ECHR.

The setting up of the VIS represents undoubtedly an important interference with the exercise of the right to privacy, if only for its scale and the categories of personal data processed. Therefore the Article 29 Working Party asked in its Opinion No 7/2004 to know 'what studies of the scale and seriousness of these phenomena revealed compelling reasons of public safety or public order that would justify such an approach'.

The EDPS has carefully taken note of the evidence presented in the EIA. Although this evidence is not fully conclusive, there appear to be sufficient reasons to justify the setting up of the VIS with the purpose of improving the common visa policy.

Within this context, it would seem to be within the margin of appreciation of the legislature to decide on the establishment of the VIS as an instrument to improve the conditions for issuing visas by Member States. Such a system could in itself well fit in and corroborate the progressive establishment of an area of freedom, security and justice as envisaged in the EC Treaty.

However, the establishment and use of the VIS could never have as an effect that a high level of protection of personal data can no longer be assured in this domain. It belongs to the advisory task of the EDPS to examine to what extent the VIS will affect the existing level of data protection of the data subjects involved.

Against this background, the EDPS will focus in this opinion on the following issues:

— the proportionality and adequacy of the data and the use thereof (e.g. categories of data, access to data for each authority concerned, and retention period);

— the operation of the system (e.g. responsibilities and security);

— the rights of the data subjects (e.g. information, possibility to correct or erase inaccurate or irrelevant data);

— the monitoring and supervision of the system.

Apart from the following paragraphs, the proposal does not give rise to important comments as to the categories of data to be included in the VIS and their use. The relevant provisions have been drafted with due care and seem to be consistent and adequate as a whole.

---

[1] 'Council Framework Decision of 13 June 2002 on combating terrorism (2002/475/JHA)' (OJ L 164, 22.6.2002, p. 3).

3.4. **Biometrics**

3.4.1. *Impact of the use of biometrics*

Using biometrics in information systems is never an insignificant choice, especially when the system in question concerns such a huge number of individuals. Biometrics are not just another information technology. They change irrevocably the relation between body and identity, in that they make the characteristics of the human body 'machine-readable' and subject to further use. Even if the biometric characteristics are not readable by the human eye, they can be read and used by appropriate tools, forever, wherever the person goes.

However useful biometrics may be for certain purposes, their widespread use will have a major impact on society, and should be subject to a wide and open debate. The EDPS must state that this debate has not really taken place before the development of the proposal. This underscores even more the need for stringent safeguards for the use of biometric data and for a careful reflection and debate in the course of the legislative process.

3.4.2. *Specific nature of biometrics*

As already underlined in several opinions of the Article 29 Working Party ([1]), the introduction and processing of biometric data for identity related documents need to be supported by particularly consistent and serious safeguards. Indeed biometric data are highly sensitive, due to some specific characteristics.

It is true that the loss of biometric data is almost impossible for person concerned, contrary to a password or a key. They offer a *quasi-absolute distinctiveness*, i.e. each individual possesses unique biometrics. They almost never change throughout a person's life which provides *permanency* to these characteristics. Everybody have the same physical 'elements' which also gives to biometrics a dimension of *universality*.

However, revocation of biometric data is almost impossible: a finger or a face is difficult to change. This positive characteristic from a number of perspectives leads to a major downside in case of *identity theft*: the storage of fingerprints and photograph in a database linked with a stolen ID could lead to major and permanent problems for the real owner of this identity. Moreover, by their very nature, biometric data are *not secret* and can even *leave traces* (fingerprints, DNA) which allow for collection of these data *without their owner being aware* of this.

Because of these risks which are inherent to the nature of biometrics, important safeguards will need to be implemented (especially in terms of respect of the purpose limitation principle, restriction of access, and security measures).

3.4.3. *Technical imperfection of fingerprints*

The main advantages of biometrics as described above (data universality, distinctiveness, permanence, usability, etc) are never absolute. This has a direct impact on the efficiency of the biometric enrolment and verification procedures planned in the regulation.

Up to 5 % of people are estimated ([2]) not to be able to enrol (because they have no readable fingerprints or no fingerprints at all). The EIA annexed to the proposal has foreseen around 20 millions visa applicants in 2007, which means that up to 1 million persons will not be able to follow the 'normal' enrolment process, with obvious consequences for the visa application and at the border checking.

([1]) Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS) (Markt/11487/04/EN - WP 96) and Working document on biometrics (MARKT/10595/03/EN - WP 80).

([2]) A. Sasse, *Cybertrust and Crime Prevention: Usability and Trust in Information Systems*, *in*'Foresight cybertrust and crime prevention project'. 04/1151, 10 June 2004, p.7, and Technology Assessment, 'Using Biometrics for Border Security', United States General Accounting Office, GAO-03-174, November 2002.

Biometric identification is also by definition a statistical process. An error rate of 0,5 to 1 % is normal ([1]), which means that the check system at external borders will have a False Rejection Rate (FRR) between 0,5 and 1 %. This rate is tuned by a threshold based on the risk policy of the competent authorities (it corresponds to a balance established between the number of persons wrongly rejected and those wrongly accepted). Therefore, it is overstated to consider that these technologies will offer an 'exact identification' of the data subject as stated in the 9th Recital of the proposed Regulation.

According to a recent prospective study ([2]) commissioned by the LIBE committee of the European Parliament, *fallback procedures* should be available to constitute essential safeguards for the introduction of biometrics as they are neither accessible to all nor completely accurate. Such procedures should be implemented and used in order to respect the dignity of persons who could not follow successfully the enrolment process and to avoid transferring onto them the burden of the system imperfections ([3]).

The EDPS therefore recommends that fallback procedures are developed and included in the proposal. These procedures should neither decrease the security level of the visa policy nor stigmatize the individual with unreadable fingerprints.

3.5. **Special categories of data**

Some categories of data (in addition to the biometric data) call for special consideration: data concerning the grounds for refusal of visa (3.4.1), and data related to other members of a group (3.4.2).

3.5.1. *Grounds for refusal of visa*

Article 10(2) of the proposal provides for the processing of data concerning the grounds for refusal, when a decision has been taken to refuse a visa. These grounds for refusal are fully standardised.

— The first two grounds in subparagraphs (a) and (b) are of a rather administrative nature: failure to submit a valid travel document, or valid documents proving the purpose and conditions of the intended stay.

— Subparagraph (c) mentions 'an alert on the applicant for the purposes to refuse entry', which implies a consultation of the SIS database.

— Finally, subparagraph (d) mentions as a reason to refuse a visa the fact that the applicant 'constitutes a threat to public policy, internal security, public health or the international relations of any of the Member States'.

([1])

Biometric	Face	Finger	Iris
FTE % Failure To Enrol	n/a	4	7
FNMR % rejection rates	4	2,5	6
FMR1 % verification match error rate	10	< 0,01	< 0,001
FMR2 % identification error rates for dB size > 1 m	40	0,1	N/A
FMR3 % screening match error rate for dB sizes = 500	12	< 1	N/A

A. K. Jain et al., *Biometrics: A grand Challenge*, Proceedings of International Conference on Pattern Recognition, Cambridge, UK., August 2004

([2]) *Biometrics at the frontiers: assessing the impact on Society*, February 2005, Institute for Prospective Technological Studies, DG Joint Research Centre, EC.

([3]) *Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data*, Council of Europe, 2005, page 11.

All grounds for refusal must be applied with great caution, because of the consequences they entail for the individual. Moreover, some of them, those in subparagraphs (c) and (d), will lead to the processing of 'sensitive data' in the sense of Article 8 of Directive 95/46/EC.

The EDPS would like to draw the attention more specifically to the condition related to public health, which seems vague and entails the processing of very sensitive data. According to the Commentary on the Articles annexed to the proposal, the reference to the threat to public health is based on the 'proposal for a Council Regulation establishing a Community Code on the rules governing the movement of persons across borders' (COM (2004)391 final).

The EDPS is aware that a 'public health' criterion is widely used in Community legislation on the free movement of persons and is applied very strictly, as shown by Directive 2004/58/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States. Article 29 of this Directive lays down the conditions for taking into account a threat to public health: 'The only diseases justifying measures restricting freedom of movement shall be the diseases with epidemic potential as defined by the relevant instruments of the World Health Organisation and other infectious diseases or contagious parasitic diseases if they are the subject of protection provisions applying to nationals of the host Member State.'

— Nevertheless, it should be noted that the proposal referred to before is, to date, only a proposal, and that the inclusion of the condition of not representing a threat to public health in the VIS Regulation is subject to the adoption of the Community Code.

— Furthermore, if it is adopted, this ground for refusing entry should be read restrictively. Indeed, the proposal for a Community Code is, in turn, based on Directive 2004/58/EC just mentioned.

The EDPS therefore recommends that a reference to Article 29 of Directive 2004/58/EC is included in text of the proposal in order to make sure that 'threat to public health' is understood in the light of that provision. In any case, considering the sensitivity of the data, they should only be processed if the threat to public health is genuine, present and sufficiently serious.

3.5.2. *Data on other members of a group*

Article 2(7) defines 'group members' as 'other applicants with whom the applicant is travelling together, including the spouse and the children accompanying the applicant'. The Commentary on the Articles mentions that the definitions in Article 2 of the proposal refer to the Treaty or the Schengen Acquis on visa policy, except for some terms, including 'group members', which are defined specifically for the purposes of this Regulation. Therefore, it can be assumed that this definition does not refer to the definition of 'group visa' as given in Article 2.1.4 of the Common Consular Instructions. The Commentary on the Articles refers to 'applicants travelling in a group with other applicants, e.g. in the framework of an ADS agreement, or together with family members'.

The EDPS stresses that a precise and comprehensive definition of 'group members' should be given in the Regulation. In the current proposal, for lack of a precise reference to the Treaty, or to the Schengen Acquis, the EDPS must observe that the definition is too vague. According to this wording, 'group members' could include colleagues, other clients from the same travel agency taking part in an organized tour, etc. The consequences are indeed very important:

according to Article 5 of the draft Regulation, the application file for an applicant will be linked to the application files of the other group members.

3.6. **Retention of data**

Article 20 of the draft Regulation provides for a five years retention period for each application file. It is a policy choice for the Community legislature to provide for a reasonable time limit.

There is no evidence — particularly not in the light of the reasons mentioned in the Commentary on the Articles — to suggest that the policy choice made in this proposal is unreasonable or would have unacceptable consequences, provided that all appropriate correction mechanisms are put into place. This means that correction or deletion of data must be ensured when the data are no longer accurate, and in particular when a person has obtained the nationality of a Member State, or has acquired a status that does not require his inclusion in the system.

Moreover, when the data are still present in the system, they can in no way prejudice a new decision. Some grounds for refusal (alert on the applicant for the purpose to refuse entry, threat to public health in particular) have a limited validity in time. The fact that they have been valid reasons to refuse entry at one moment should not influence a new decision. The situation must be entirely re-assessed for each new visa application and this should be made explicit in the Regulation where appropriate.

3.7. **Access and use of data**

3.7.1. *Preliminary observations*

As a preliminary remark, the EDPS recognizes the care which has obviously been devoted to the regulatory system of access and use of the VIS data. Each authority has access to different data for different purposes. This is an appropriate approach that the EDPS can only encourage. The following observations aim at applying this approach to the fullest extent.

3.7.2. *Checks on visas at external border checkpoints and within the territory*

In the case of visa checks at external borders, Article 16 of the proposed Regulation enounces clearly the two exact purposes:

— 'verifying the identity of the person', which means according to the given definition, a 'one to one' comparison;

— 'verifying the authenticity of the visa'. As proposed by the ICAO standards, the microchip of the visa could use a public/private key system (PKI) in order to conduct this authentication process.

These two purposes can properly be reached with the sole access to the protected microchip by the competent authorities for carrying out checks on visas. An access to the central database of the VIS would therefore be disproportionate in this specific case. This latter option would involve more authorities connected to the VIS, which might increase the risk of misuse. It might also be a more expensive option as the number of secure and controlled access to the VIS, and the need for specific training related to this access will significantly increase as well.

Furthermore, there are doubts as to the adequacy of the access to the data as foreseen in the second point of Article 16. Indeed, paragraph (2)(a) states that if, after a first query, it appears that data on the applicant is recorded in the VIS (which should be the case in principle), the competent authority can consult other data, still for the purpose of verifying the identity. These data concern all information related to the application, photographs, fingerprints, as well as any visa previously issued, annulled, revoked or extended.

If the verification of identity has succeeded, it is not clear at all for what reason the rest of these data are still needed. They should actually only be made accessible, under restrictive conditions, if the verification procedures have failed. In this case, the data mentioned in Article 16(2) would appropriately contribute to a fallback procedure helping to ascertain the identity of the person. They should then not be accessible to each border checkpoint staff, but only more restrictively to officials in charge of difficult cases.

Finally, the definition of the authorities having access should be more precise. In particular, it is not clear what the 'competent authorities for carrying checks within the territory of the Member State' are. The EDPS assumes it concerns the competent authorities for carrying out checks *on visas*, and Article 16 should be amended in this sense.

3.7.3. *Use of data for identification and return of illegal immigrants, and for asylum procedures*

In the cases described by Articles 17, 18 and 19 (return of illegal immigrants and asylum procedure), the VIS is used for the purpose of identification. Among the data which can be used for identification purposes are the photographs. However, in the current state of the technology related to automated facial recognition for such large scale IT systems, photographs cannot be used for identification (one-to-many); they cannot provide for a reliable result. They are therefore not to be considered as data adequate for the purpose of identification.

Consequently, the EDPS strongly suggests that the 'photographs' be removed from the first part of these articles and maintained in the second part (photographs can be used as a tool for verifying someone's identity, but not to identify in a large scale database).

An other option would be to amend Article 36 in the sense that the functionalities for processing photographs for identification purposes will only be implemented when this technology is considered reliable (possibly after advice from the technical committee).

3.7.4. *Publication of the authorities having access*

Article 4 of the draft Regulation provides for a publication in the *Official Journal of the European Union* of the competent authorities designated in each Member State to have access to the VIS. This publication should be made on a regular (annual) basis, in order to inform about the changes in national situations. The EDPS stresses the importance of this publication as an indispensable tool for control, at a European as well as at national or local level.

3.8. **Responsibilities**

It is recalled here that the VIS will be based on a centralised architecture with a central database where all information on visa will be stored and national interfaces located in the Member States allowing their competent authorities to access the central system. According the recitals 14 and 15 of the draft Regulation, Directive 95/46/EC will apply to the processing of personal data by the Member States in application of the Regulation, and Regulation 45/2001 will apply to the activities of the Commission in relation to the protection of personal data. As mentioned in these recitals in this context, the proposal aims to clarify certain points, *inter alia*, in respect of the responsibility for the use of the data and of the supervision on data protection.

In fact, these points would seem to relate to some crucial details without which the system of safeguards in Directive 95/46/EC and Regulation 45/2001 would not apply or would not be fully consistent with the proposal. The applicability of national law under the Directive normally assumes a controller which is established in that Member State (Article 4), whereas the applicability of the Regulation depends on the processing of personal data by a Community institution or body in the exercise of activities all or part of which fall within the scope of Community law (Article 3).

According to Article 23(2) of the draft Regulation, the data shall be 'processed by the VIS on behalf of the Member States'. According to Article 23(3) the Member States shall designate the authority considered as controller in accordance with Article 2(d) of Directive 95/46/EC. This seems to suggest that, according to the system of the Directive, the Commission should be regarded as a processor. This is confirmed by the Explanation of the Articles ([1]).

This language tends to understate the very important and in fact crucial role of the Commission, both in the development phase of the system and in the course of its normal operation. It is difficult to link exactly the Commission's role to the concept of controller or processor; it is either a processor with unusual powers (among others in designing the system), or a controller with restrictions (since the data are entered and used by Member States). The Commission really has what must be recognized as a *sui generis* role ([2]) in the VIS.

This significant role should be recognized through a comprehensive description of the Commission's tasks, rather than through a wording that does not quite correspond to the reality, because it is too restrictive, does not change anything in the operation of the VIS and only leads to confusion. This is also important with a view to a consistent and effective supervision of the VIS (see also paragraph 3.11). Therefore, the EDPS recommends to delete Article 23(2).

The EDPS would like to emphasize that a complete description of the tasks of the Commission with regard to the VIS is all the more important, if the Commission envisages entrusting the management tasks to another body. The 'Fiche Financière' annexed to the proposal mentions the possibility to transfer these tasks to the external border agency. In this context, it is crucial that the Commission does not leave any uncertainty as to the scope of its competences, in order for its successor to know the boundaries within which he can act.

3.9. **Security**

The management and respect of an optimal security level for the VIS constitutes a precondition for ensuring the required protection of personal data stored in its database. In order to obtain this satisfactory level of protection, proper safeguards have to be implemented for handling the potential risks related to the infrastructure of the system and to the persons involved. This subject is now discussed in various parts of the proposal and deserves some improvement.

Articles 25 and 26 of the proposal contain various measures for data security and specify the kind of misuses that need to be prevented. These provisions could, however, be usefully complemented by measures to systematically monitor and report on the effectiveness of the security measures that have already been mentioned. The EDPS recommends more specifically that provisions on systematic (self-)auditing of security measures are added to these articles.

This is linked to Article 40 of the proposal, which provides for monitoring and evaluation. This 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. The EDPS therefore recommends that the scope of Article 40 is extended to monitoring and reporting on the lawfulness of processing.

Moreover, in complement to Article 24(4)(c) or Article 26(2)(e) concerning the duly authorised staff which has access to the data, it should be added that Member States should ensure that precise user profiles are available (that should be kept at the disposal of the national supervisory authorities for checks). In addition to these user profiles, a complete list of user identities has to be made and kept permanently up-to-date by Member States. The same applies to the Commission: Article 25(2)(b) should therefore be complemented in the same sense.

([1]) See page 37 of the proposal.

([2]) Although the definition of controller in Directive 95/46/EC and Regulation 45/2001 also provides for the possibility of more controllers with different responsibilities.

These security measures are completed by monitoring and organisational safeguards. Article 28 of the proposal describes the conditions and the purposes for which records of all data processing operations have to be kept. 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 effective execution of the tasks of the supervisory authorities that will be able to identify the weakest spots and to focus on them during their own auditing procedure.

3.10. **Rights of the data subject**

3.10.1. *Information of the data subject*

Providing information to the data subject to ensure fair processing is of the greatest importance. It constitutes an indispensable safeguard for the rights of the individual. Article 30 of the proposal now basically follows Article 10 of Directive 95/46/EC for that purpose.

This provision could, however, benefit from some amendments in order to make it better fit into the framework of the VIS. The Directive provides indeed for certain information to be given, but allows for more information to be given if appropriate ([1]). Consequently, Article 30 should be amended in order to include the following points:

— Data subjects should also be informed about the retention period applying to their data.

— Article 30(1)(e) concerns 'the right of access to, and the right to rectify the data'. It would be more accurate to mention 'the right to access, and the right to *request* rectification *or deletion* of the data'. In this regard, data subjects should be informed of the possibility to apply for advice or assistance to the relevant supervisory authorities.

— Finally, Article 30(1)(a) mentions the information about the identity of the controller, and of his representative, if any. The controller being always installed on the territory of the European Union, there is no need to foresee this latter possibility.

3.10.2. *Rights of access, correction and deletion*

Article 31(1) last sentence states that 'such access to data may be granted only by a Member State'. It can be assumed that this means that access to (or communication of) the data cannot be granted by the Central Unit, but by any Member State. The EDPS recommends that it is made explicit that such communication can be requested in any Member State.

Moreover, the drafting of this provision also seems to imply that access cannot be denied, and will be given without authorization of the Member State responsible. That would explain why national authorities have to cooperate to enforce the rights laid down in Article 31(2), (3) and (4) but not in Article 31(1) ([2]).

3.10.3. *Assistance by supervisory authorities*

Article 33.2 lays down that the obligation of the national supervisory authorities to assist and advise the person concerned subsists throughout proceedings (before a court). The meaning of this paragraph is not clear. The national supervisory authorities have different attitudes towards their role during court proceedings. This sounds as if they have to play the role of the counsel of the complainant in court, which is not possible in many countries.

([1]) It mentions *'any further information (…) insofar as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject'*.

([2]) Consequently, Article 31(3) concerning cooperation between national authorities in the exercise of the rights of correction or deletion could be amended in this sense, for more clarity: 'if the request *as mentioned in 31(2)*' The requests as mentioned in 31(1) (access) do not involve cooperation between authorities.

3.11. **Supervision**

The proposal shares out the supervisory task between national supervisory authorities and the EDPS. This is consistent with the approach of the proposal to applicable law and responsibilities for the operation and use of the VIS, and with the need for an effective supervision. The EDPS therefore welcomes this approach in Articles 34 and 35.

The national supervisory authorities monitor the lawfulness of the processing of personal data by the Member States, *including their transmission to and from the VIS*. The EDPS monitors the activities of the Commission *(…) including that the personal data is transmitted lawfully between the National Interfaces and the Central Visa Information System*. This might result in overlapping, as both the national supervisory authority and the EDPS are at the same time responsible for monitoring the lawfulness of transmission of data between the National Interfaces and the Central Visa Information System.

The EDPS therefore suggests an amendment of Article 34 in order to clarify that the national supervisory authorities monitor the lawfulness of the processing of personal data by the Member State, including their transmission to and from the National Interface of 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 the EDPS should be coordinated to a certain extent, in order to ensure a sufficient level of consistency and overall effectiveness. Indeed, there is a need for a harmonized implementation of the Regulation, and for working towards a common approach of common problems. Moreover, as security is concerned, it can be added that the security level of the VIS will — ultimately — be defined by the security level of its weakest link. In this regard also the cooperation between the EDPS and the national authorities needs to be structured and enhanced. Article 35 should thus contain a provision to that effect setting out that the EDPS shall convene a meeting with all national supervisory authorities, at least once a year.

3.12. **Implementation**

Article 36(2) of the proposal provides: '*The measures necessary for the technical implementation of the functionalities referred to in paragraph 1 shall be adopted in accordance with the procedure referred to in Article 39(2).*' Article 39 refers to a committee for assisting the Commission which was created in December 2001 ([1]) and has been used in several instruments.

The technical implementation of the VIS functionalities (interactions with the competent authorities and the uniform format of visa) presents a number of potential critical impacts on data protection. For instance, the choices to embed a microchip or not in the visa which will have an impact on the way the central database will be used, as well as the standard of the format used to exchange biometric data will drive or design the related data protection policy ([2]).

This selection of technologies will have a determinant impact on the proper implementation of the principles of purpose and proportionality, and should consequently be supervised. Therefore, technological choices with a substantial impact on data protection should preferably be made by way of Regulation, in accordance with the co-decision procedure. Only then, the necessary political control can be given. In all other cases with an impact on data protection, the EDPS should be given the possibility to advise on the choices made by this committee.

3.13. **Interoperability**

Interoperability is a critical and vital precondition for the efficiency or large scale IT systems as the VIS. It offers the possibility to reduce the overall cost in a consistent manner and to avoid natural redundancies of heterogeneous elements. Interoperability can also make a contribution to the objective of a common visa policy by implementing the same procedural standard to all the constitutive elements of this policy. However, it is crucial to distinguish between two levels of interoperability:

— Interoperability between EU member states is highly desirable; indeed the visa applications sent by one Member State's authorities have to be interoperable with the ones sent by any other Member State's authorities.

([1]) Council Regulation (EC) No 2424/2001 of 6 December 2001 on the development of the second generation Schengen Information System (SIS II).

([2]) The proposal for a Council regulation amending (EC) No 1683/95 (uniform format for VISA) in September 2003 included also a similar article.

— Interoperability between systems built for different purposes or with third country systems is far more questionable.

Among the available safeguards used to limit the purpose of the system and prevent 'function creep', the use of different technological standards can contribute to this limitation. Moreover, any form of interaction between two different systems should be thoroughly documented. Interoperability should never lead to a situation where an authority, not entitled to access or use certain data, can obtain this access via another information system.

In this context, the EDPS would like to refer to the Declaration of the Council of 25 March 2004 on Combating Terrorism, in which the Commission is asked to present proposals in order to enhance interoperability and synergies between information systems (SIS, VIS and Eurodac).

He would also like to refer to the ongoing discussion as to which body could be entrusted with the management of the different large scale systems in the future (see also paragraph 3.8 of this opinion).

The EDPS wants to stress again that interoperability of the systems can not be implemented in violation of the purpose limitation principle, and that any proposal in this matter should be submitted to him.

4. **CONCLUSIONS**

4.1. **General points**

1. The EDPS recognises that the further development of a common visa policy requires an efficient exchange of relevant data. One of the mechanisms that can ensure a smooth flow of information is the VIS. The EDPS has carefully taken note of the evidence presented in the EIA. Although this evidence is not fully conclusive, there appear to be sufficient reasons to justify the setting up of the VIS with the purpose of improving the common visa policy.

   However, this new instrument should be limited to the collection and exchange of data, as far as such a collection or exchange is necessary for the development of a common visa policy and is proportionate to this goal.

2. The establishment of the VIS may have positive consequences for other legitimate public interests, but this does not alter the purpose of the VIS. Therefore all the elements of the VIS must be necessary and proportional instruments to reach the policy goal, mentioned above. Moreover:

   — Routine access by law enforcement authorities would not be in accordance with this purpose.

   — The EDPS recommends that this distinction between 'purpose' and 'benefits' is made more explicit in the text of Article 1(2).

   — Interoperability with other systems can not be implemented in violation of the purpose limitation principle.

3. The EDPS recognises the advantages of the use of biometrics, but stresses the major impact of the use of such data and suggests the insertion of stringent safeguards for the use of biometric data. Moreover, the technical imperfection of fingerprints requires that fallback procedures are developed and included in the proposal.

4. The present opinion should be mentioned in the preamble of the Regulation before the recitals ('Having regard to the opinion …').

4.2. **Other points**

5. Concerning the grounds for refusal of visa: a reference to Article 29 of Directive 2004/58/EC should be included in the text of the proposal in order to make sure that 'threat to public health' is understood in the light of that provision.

6. Data on members of a group have a special meaning in the proposal: therefore a precise and comprehensive definition of 'group members' should be given.

7. There is no evidence that the policy choice made in this proposal on the delay on the retention of data is unreasonable or would have unacceptable consequences, provided that all appropriate correction mechanisms are put into place.

   Moreover, it should be made explicit in the proposal that personal data must be entirely re-assessed for each new visa application.

8. Concerning visa checks at external borders: Article 16 of the proposal should be amended since an access to the central database of the VIS would be in those cases disproportionate. A sole access to the protected microchip by the competent authorities for carrying out checks on visas is sufficient.

   Moreover, if the verification of identity has succeeded, it is not clear at all for what reason the rest of these data are still needed.

9. Concerning the use of data for identification and return of illegal immigrants, and for asylum procedures: 'photographs' should be removed from the first part of the Articles 17, 18 and 19 and maintained in the second part.

10. Concerning the responsibilities of the Commission and the Member States: Article 23(2) should be deleted.

11. Provisions on systematic (self-)auditing of security measures should be added to the proposal. The scope of Article 40 must be extended to monitoring and reporting on the lawfulness of processing. Moreover:

   — a complete list of user identities has to be made and kept permanently up-to-date by Member States. The same applies to the Commission: Article 25(2)(b) should therefore be complemented in the same sense.

   — Article 28 of the proposal describes the conditions and the purposes for which records of all data processing operations have to be kept. 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.

12. Concerning the rights of the Data Subject:

   — Article 30 should be amended in order to assure that Data subjects should also be informed about the retention period applying to their data.

   — Article 30(1)(e) should mention 'the right to access, and the right to request rectification or deletion of the data'.

   — Article 31(1) must make explicit that certain communications can be requested in any Member State.

13. Concerning supervision:
    - Article 34 should be amended in order to clarify that the national supervisory authorities monitor the lawfulness of the processing of personal data by the Member State, including their transmission to and from the National Interface of the VIS.
    - Article 35 should thus contain a provision setting out that the EDPS shall convene a meeting with all national supervisory authorities, at least once a year.
14. Concerning implementation:
    - Technological choices with a substantial impact on data protection should preferably be made by way of Regulation, in accordance with the co-decision procedure.
    - In other cases, the EDPS should be given the possibility to give advice on the choices made by the committee foreseen by the proposal.

Done at Brussels on 23 March 2005.

Peter HUSTINX

European Data Protection Supervisor