ARTICLE 29 Data Protection Working Party

1022/05/EN
WP 110

Opinion 2/2005

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)

Adopted on 23 June 2005

Table of contents

Opinion 2/2005
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)

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

Having regard to Article 29, Article 30(1)(c) and Article 30(3) of the above Directive,

Having regard to its rules of procedure, and in particular Articles 12 and 14 thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction

1.1. Dimension of the project and its impact

The project of setting up a central database and a system of exchange of information concerning short-stay visas raises important questions for fundamental rights and freedoms of individuals and in particular their right to privacy.

It will lead to a massive collection and processing of personal and biometric data, their storage in a centralised database and to large scale exchanges of information concerning a huge number of persons.

Data Protection Authorities are particularly concerned about the potential risks of such a project and stress the importance of ensuring proper respect for the principles of data protection.

The question of necessity and proportionality of such a large database, in particular with respect to the choice of integration of biometric data held in the system has been publicly discussed several times.

1.2. Background of the proposal

The establishment of the Visa Information System (VIS) as a system for the exchange of visa data between Member States is one of the key elements for the implementation of a common visa policy with the view to achieving the objectives set out in Article 61 of the Treaty on the European Community (TEC), namely the free movement of persons in an area of liberty, security and justice. The Commission has been working along the guidelines set by the JHA

[1] Official Journal no. L 281 of 23/11/1995, p. 31, available at: http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm.

Council on 19 February 2004[2]. In these conclusions, the Council asked the Commission in particular to fully respect the Communities' legislation on the protection of personal data when preparing the technical implementation of the VIS and the proposal for the legal instrument concerning the establishment of the VIS.

Decision 2004/512/EC, adopted by the Council of the EU on June 8, 2004[3] provided the legal basis for setting up the VIS system and allowed for the inclusion in the Community budget of the necessary appropriations for the technical development of the system.

On December 28, 2004 the Commission submitted the current 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.[4]

The proposal gives the Commission the mandate to set up, maintain and operate the VIS and defines the purpose, functionalities and responsibilities for the Visa information system and the procedures and conditions for the exchange of data between Member States.

The development and establishment of the VIS requires, as clarified in the explanatory memorandum annexed to the Proposal, a comprehensive legal framework, including in particular the

- Amendment to the Common Consular Instructions (CCI)[5] on visas for the diplomatic missions and consular posts of the Contracting Parties to the Schengen Conventions,
- Development of a mechanism for the exchange of data with Ireland and the United Kingdom (which do not participate in the Schengen system) in order to facilitate the application of the Dublin II Regulation and assist in the identification and administrative procedures for returning of illegal immigrants.
- Exchange of data on long stay visas, as per Article 63 of the TEC, currently not included in the common visa policy.[6]

Other measures may also be necessary in order to achieve free movement of persons throughout the European Union, including the waiving of controls at the internal borders and strengthening those controls at the external borders. They are indeed contained in a proposal for a Regulation establishing a Community Code on the rules governing the movement of persons across borders[7].

It is also appropriate to mention the on-going activities aimed at the development of the Schengen information system, the so called SIS II. On the 31st May a Draft Decision and Draft Regulation were submitted by the Commission envisaging amendments to the provisions of the Schengen Convention concerning the Schengen Information System (SIS) and introducing new functions in the system as well as new data categories; the number and

[2] Council Document 6535/04 VISA 33 COMIX 111

[3] Council decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC)- OJ L 213, 15.6.04, p. 5.

[4] Document COM(2004)835-Final, not yet published in the Official Journal of the EU.

[5] Common Consular Instructions on Visas for the Diplomatic Missions and Consular Posts, OJ C310/1, 19.12.03.

[6] The common visa policy as defined within the framework of the Member States that have set up a regime of free movement of individuals in their respective territories, by abolishing internal borders, is regulated by Article 62 of the Treaty and only applies to short-stay visas (i.e. for periods not exceeding three months); such visas are issued on the basis of common rules and a uniform model (so-called uniform (or Schengen) visa)..

[7] COM (2004) 0391 of 26.05.2004, which will replace the corresponding provisions of the Schengen Convention. It was not submitted to the WP29 for opinion.

categories of authority allowed to access the system are also to be expanded.[8] Currently, "visa authorities" may access the SIS, in particular the alerts based on Article 96 of the Convention in respect of non-admissible foreigners.

Additionally, it should be considered that in a proposal for a Regulation submitted by the Commission in December 2003, which has not yet been finally adopted by the Council, a uniform format was devised for visa (and residence permit) applications; the insertion of two items of biometric data should be mandatory for applicants: a digital photograph of the holder and the digital images of the holder's fingerprints (two fingers), both to be stored on a microchip[9]. This provision would appear to supplement the insertion of the said data into the VIS, and is especially important with regard to the use of data for border check that is mentioned in Article 16 of the Proposal.

The VIS will be composed of a central structure and national interfaces and will be supplemented by the establishment, at domestic level, of the corresponding national systems including stable computerised links with consulates and border checkpoints of each participating country; it will contain, in addition to alphanumeric data on applicants for short-stay visas (uniform visas), biometric data, in particular the visa applicants fingerprints collected upon submitting a visa application.

Establishment and operation of the VIS according to the initial project were expected to take place in two stages: an initial one as for alphanumeric data, and a subsequent stage related to the entering of biometric data into the system..

The Conclusions of the JHA Council of 19 February 2004 state that at a later stage, in line with the choice of biometrics in the field of visas and taking into account the outcome of the on-going technical developments, biometric data on visa applicants should be added to the VIS.

In February 2005, the Council, taking into account the technical problems linked to the inclusion of biometric data on visa, which have delayed the adoption of the Regulation, invited the Commission to make every effort" including, with respect to budgetary programming, to bring the activation of biometric identifiers in the development of the central part of the VIS forward to 2006"[10]. It should be pointed out that this imposes no obligation on the Commission, therefore it does not entail, as such, the need for amending Article 36(2) of the Proposal.

Furthermore, given the approach followed by the Council and in order to ensure consistency as regards the introduction of biometric data in the VIS, an appropriate legal basis is necessary in order to introduce the obligation to provide those data.

To that end, the Commission envisages an additional, specific measure, i.e. a draft Regulation adapting the Common Consular Instructions. This new instrument, as clarified in the Explanatory Memorandum, will concern, in particular, "standards and procedure for taking the biometric data, including the obligation and specifying the exception to the recording of biometrics".

[8] Proposal for a Council Decision on the establishment, operation and use of the second generation Schengen information system (SIS II) [COM (2005) 230 final]; and Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II) [COM (2005) 236 final].

[9] Draft Council Regulation amending Regulations 1683/95 and 1030/2002 laying down a uniform format for visas and for residence permits for third country nationals.(COM (2003) 558 final, 24.9.2003).

[10] Draft Council Conclusions as contained in document 6492/05 of 17 February 2005.

The introduction of this new obligation is an addition to the requirement set out in the draft Regulation concerning the VIS; therefore, the references in the current proposal to the inclusion and use of biometric data must be read as being dependent on the entry into force and effective implementation of the corresponding obligations on Member States pursuant to the adoption of the Regulation containing the adaptation of the CCI .

1.3. Description of the current proposal

The VIS system is aimed at exchanging visa data between those Member States "which have abolished checks at their internal borders" and participate "in the system of free movement without checks at internal borders"; the relevant legal basis has been found in Articles 62, 2, b, ii) and 66 of the TEC.

In the Proposal, it is specified that it constitutes a measure to support the common visa policy, and thus a development of the Schengen acquis

The proposal lays down detailed provisions on the system and its operation, lists the categories of data to be entered into the system, the authorities of Member States that may enter data in the system as well as access the data contained therein, the retention period for the data, the right of access and the rights of correction and deletion of the person concerned (i.e. the data subject), the security measures to be adopted and the supervision at EU and national level.

As for its structure, the Visa Information System, in line with the Council decision, has been designed in accordance with a centralised architecture consisting of a central information system, "the Central Visa Information System" (CS-VIS), including the information set forth in Articles 5 to 12 of the Draft Regulation; an interface in each Member State, "the National Interface" (NI-VIS), which shall provide the connection to the relevant central national authority of the respective Member State; and the communication infrastructure between the Central Visa Information System and the National Interfaces. The on-going creation of the VIS is based on a common technical platform with the enhanced Schengen Information System – the so-called "SIS II"[11].

The synergies with the Schengen system are also highlighted by the decision whereby the Commission, in exercising the authority committed to it, would be assisted by the Committee set up by Article 5(1) of Council Regulation No. 2424/2001 of 6 December 2001 – i.e. the so-called SIS II Committee.

The financial schedule to the proposal specifies that the system shall be set up and maintained by the Commission and that the latter shall be responsible for operating the Central Visa information system and the communication infrastructure between the Central Visa information system and the National Interfaces. The data will be entered and processed in the VIS under the Member States' responsibility. The Commission undertakes responsibility for the "technical" management of the system.

The system capability is estimated – in particular as regards biometric data – to be able to contain, as of 2007, the data concerning about 20 million of visa applications annually, which would result into 70 million of fingerprints data to be stored in the system for the five-year term set forth in the proposal; the 70 million figure is estimated by taking a 30% of "frequent travellers" off the total.

[11] Which is to include additional functions and categories of data compared with the current SIS by also integrating the new Member States following enlargement of the EU with reference to the new proposal for regulation on SIS II. See also footnote n° 8.

The financial costs to ensure system operation have been estimated (and apportioned) on the basis of the aforementioned financial schedule; in the 2007-2013 period, they will amount to 153 million euro, of which over 70% will cover the processing of biometric data in the system.

To the figures and configuration described above, there should be added those related to the national portion of the VIS. According to Article 2(2) of Decision 2004/512 EC, the national infrastructures beyond the national interfaces in the Member States shall be adopted and developed by each Member State. This includes the financial burden for the development of these infrastructure and the adaptation of existing national systems to the VIS, the world-wide connections to their consular posts, (including border points and other points of control referred to in Article 16 of the proposal) and their equipment, shipping and training.

1.4. Previous opinion of the Working Party

The Article 29 Working Party has rendered an Opinion on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)[12], highlighting the principles underlying the conditions on which a database of this kind should operate, exactly with a view to providing useful guidance to both the Commission and the SIS II consultative Committee in view of their forthcoming proceedings.

The Commission has formally requested the WP' Opinion on the Proposal for a Regulation.

The draft Regulation contains a number of provisions dealing with data protection principles.

However, fundamental features of the VIS such as the specific definition of the purposes of the system and the entities responsible for the processing of the data (data controllers), proportionality of the data to be collected and retention periods, application of the transparency principle, and more detailed specification of supervision and control tasks at both central and national level might be improved further in the light of the considerations made in the following paragraphs.

2. Analysis of the Proposal

On the basis of the considerations already referred to in part, the Working Party holds the view that the importance and special complexity of the issues at stake require an articulated opinion to supplement the points raised in the said Opinion no. 7/2004.

2.1. General considerations

This initiative has a major impact on the fundamental rights of a large and rapidly growing number of persons, as it envisages that all the applications submitted to the States that avail themselves of the VIS to grant any of the short-stay visas listed in Article 2 will have to be entered in the VIS on a mandatory basis; furthermore, links will be established with other applications possibly submitted by the same individual and already recorded in the VIS as well as with the data of individuals travelling in a group and with people providing accommodation in the EU countries requiring the visas..

[12] Opinion No. 7/2004 WP96 of 11.08.04, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_en.pdf

The system is to include alphanumeric data concerning each application as well as a broad range of information, including in particular data related to the applicants' photographs and fingerprints.

Size and capability of this system are currently unrivalled in the EU, with the potential of collecting 70 millions of personal data in 5 years' time.

Similarly wide-ranging mechanisms have been envisaged in respect of both access to the system and the scope of the authorities enabled to perform such access, even though attempts at restricting this scope have been made in the draft Regulation.

Another feature potentially enhancing accesses – therefore the use of the system for multiple purposes – is related to the objective of achieving "enhanced interoperability between European databases" and creating synergies between, namely, SIS II, VIS and Eurodac. The draft Regulation does not contain specific rules applying to collection of the data on the individuals to be included in the system. Article 3 provides that the following categories of data should be stored in the VIS: alphanumerical data of the applicant and on visas, photograph, fingerprint data, links to other applications.

Collection and insertion of personal data may be only carried out by the authorities and for the purposes referred to in the instrument setting up the VIS, in compliance with the principles of the Directive; the proposal at issue should contain specific provisions in this regard to clarify the scope of the restrictions imposed on individual rights and freedoms, and in particular on the right to personal data protection.

a) Necessity criterion

Processing of the data will have to be consistent with the principles of data protection and protection of privacy enshrined in Article 8 of the Charter of Fundamental Rights of the EU and referred to both in Directive 95/46/EC and in national legislation. It is necessary to ensure the "right to respect for private and family life" set forth in Article 8 of the European Human Rights Convention, which provides – partly in the light of the relevant case law of the European Court of Human Rights– key guidance to clarify the limitations posed on interferences with an individual's private sphere by public authorities exercising the powers conferred on them. Article 8 (2) of the ECHR provides that interferences are only to be allowed on condition that they are in accordance with the law and are necessary, in a democratic society, to protect an important public interest.

The European Court of Justice has made clear that these criteria apply when assessing whether processing of personal data is in conformity with Community Law[13].

It is necessary for the interference to be legitimate to have, on the one hand, an appropriate legal basis in law, and on the other hand, that this "law" satisfies certain quality requirements.

[13] Judgment of the Court of 20 May 2003 joined cases C-465/00, C-138/01 and C-139/01 (Rechnungshof), in particular paragraphs 72 and 83:
72 So, for the purpose of applying Directive 95/46, in particular Articles 6(1)(c), 7(c) and (e) and 13, it must be ascertained, first, whether legislation such as that at issue in the main proceedings provides for an interference with private life, and if so, whether that interference is justified from the point of view of Article 8 of the Convention.
83 According to the European Court of Human Rights, the adjective `necessary' in Article 8(2) of the Convention implies that a `pressing social need' is involved and that the measure employed is `proportionate to the legitimate aim pursued' (see, inter alia, the Gillow v. the United Kingdom judgment of 24 November 1986, Series A no. 109, § 55). The national authorities also enjoy a margin of appreciation, `the scope of which will depend not only on the nature of the legitimate aim pursued but also on the particular nature of the interference involved' (see the Leander v. Sweden judgment of 26 March 1987, Series A no. 116, § 59).

The conditions for the exercise of powers by public authorities must be precisely defined, so as to restrict arbitrarily in the exercise of public power, and rules must be easily available in order to allow the individual to adjust his behaviour accordingly.

A "*pressing social need*" is to be involved and it is not sufficient that some functionalities be merely "useful", as they must be necessary - which implies that without them the objectives cannot be reached.

The measure employed is to be also "proportionate to the legitimate aim pursued".

The respect of these conditions is of utmost importance in the present case and this imposes the need to avoid vague or broadly-worded concepts in the proposal.

It is necessary, therefore, to specify the aim that is pursued by the draft Regulation, and assess proportionality of the data to be entered in the system by having regard to the said aim.

Account must be taken of the processing as a whole, therefore of the functions envisaged for the database in question. For each of these functions, it will be necessary to establish whether the processing and its mechanisms, the categories of the data to be collected and processed, the authorities allowed to access the information contained in the database, and the security measures to be adopted are necessary and indispensable as resulting from "a pressing social need"; further, it will be necessary to consider the rights to be granted to the individuals the personal data refer to, and ensure a proper mechanism to exercise such rights.

b) Legal basis

It should be clarified whether the obligation to provide those data requires a further specific, detailed legal instrument, or whether the Proposal in itself may be considered as an adequate legal framework. The latter view would appear to be held by the Commission, providing that it will present a proposal for an amendment to the Common Consular Instructions concerning in particular standards and procedure for the "collection of personal data". Clarification is appropriate both in order to strengthen the decision-making process of the Proposal and to allow evaluating compliance with purpose specification and proportionality principles.

In this manner it will be possible to highlight how the Proposal relates to and is consistent with other draft regulations submitted by the Commission and currently discussed in the Council.

In the light of the decision of the Council to anticipate the inclusion of biometric data in the VIS, specific, additional considerations should be made to also address the existing legal framework in the Schengen area as the issuance of short-stay visas.

The reference to the Common Consular Instructions should be clarified also to assess whether the latter may be regarded as such to provide the appropriate legal basis to allow collecting personal data in compliance with Article 6 of the Directive..

2.2. Proportionality and purpose limitation

Consideration of the purpose(s) of the processing is paramount in assessing adequacy and proportionality of the proposed measures, which is a requirement in order for any interference in the fundamental right to privacy to be legitimate and it is essential in respect of the lawfulness criteria set out in Article 6 of EC Directive 95/46/EC, which applies to the draft Regulation, whereby personal data must be collected only for *specified, explicit and legitimate purposes*, may not be further processed in a way that is *incompatible with those*

purposes, must be adequate, relevant and not excessive *in relation to the purposes* for which they are collected and further processed.

It is essential to lay down the specific purposes to be pursued via the VIS in order to evaluate whether the proportionality principle has been complied with. This calls in the first place for a clear-cut, narrow definition of the purposes of the intended processing.

The Proposal indicates in Article 1, paragraph 2 the objectives of VIS as a means to "improve the administration of the common visa policy, consular cooperation and consultation between central consular authorities", however the text as subsequently worded would appear to refer to other purposes (see letters a) to f) of the same paragraph) which should be set out clearly in relation to the legal basis for the proposal.

Some of these purposes might actually be pursued by means of the Schengen information system (SIS); therefore it is necessary not to give rise to overlapping and/or duplications between the two systems.[14]

The reference to "*fight against fraud*", "*prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application* may be regarded as other legitimate "benefits" and seems consistent with the legal basis chosen by the Commission.

The need for foreseeability and availability of the Law pursuant to Article 8 ECHR impose that such criteria should be clearly available to the public in an easy way, either through their inclusion as part of the regulation or through an appropriate reference to the source where they can be found.

As far as the reference to "*threats to internal security*" is concerned, this seems to be a broad, cross-sectoral purpose, which is already pursued by the many tools available for police cooperation - including the SIS – and must be referred to only in the light of the main purpose of the VIS - which is and must remain that of improving the common visa policy, and therefore may only be deployed insofar as it is compatible with the said policy.

"*facilitate checks at external border and within the territory*"; "*assist in the identification and return of illegal immigrants*"; "*facilitate the application of Regulation (EC) No. 343/2003*"; these purposes would not appear to be in line with the first requirement set forth in Article 8 of the ECHR, as they are not included in the measures that may be adopted by having regard to the legal basis underlying the proposal.

On the other hand, different "purposes" for certain processing operations are mentioned throughout the proposal ("purpose of examination of applications", Article 13; "purposes of consultation between authorities", Article 14; "purposes of reporting and statistics", Article 15; "purposes of identification", Article 16 and 17). This multiplicity of "purposes" should be reconsidered in order to meet specific requirements that should not be in contradiction with the essence of the purpose limitation principle.

In the light of Article 6 of the Directive, the "purposes" of the data processing involved should be closely defined and limited to the need for improving the common visa policy, and that the wording of the proposal should be amended accordingly. The purpose of the processing would be in line with the legal bases used by the Commission to put forward its proposal, namely Article 62.2.b, ii and Article 66 TEC.

[14] The SIS II system is currently under construction as well, and reference is be made here to the concerns voiced in its respect by the Schengen Joint Supervisory Authority in an opinion issued in April 2004.

2.3. Categories of data involved

The current proposal provides for the inclusion in the VIS of different data categories, including biometric data.

Article 6 of Directive 95/46/CE sets forth the principle that personal data may be legitimately processed only if they are adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

The inclusion of personal data in the system can be done on the basis of a specific legislation providing for the mandatory submission by the applicant of a visa of the information considered necessary for the procedure of granting a visa and in order to avoid visa shopping and fraud.

Even assuming the VIS to be built on a set of pre-existing rules – which actually are not always publicly known and/or specified clearly -, i.e. assuming that it refers to data requested from applicants at the time of submitting their visa applications, compliance with the Directive requires careful evaluation of the need for including such data into the system.

Depending on the mechanism for access to and communication/dissemination of the data, or else on the retention period, some personal data may prove especially intrusive; it is therefore necessary to apply a strict selective approach so as to include the data that are actually essential to achieve the purposes referred to above, i.e. the development of the common visa policy. Any other data, providing they are necessary, may be exchanged by using, in particular, the channel of co-operation between central authorities, as foreseen in Article 7 of the proposal.

a) Applicant's nationality at birth

The WP considers in that respect that the applicant's nationality at birth (in addition to the current one) as requested in Article 6 is of no relevance to the implementation of the common visa policy and may actually give rise to unlawful discrimination between applicants that are nationals of the same third country. The Working Party therefore requests its deletion from Article 6.

The need to make available this data in specific cases should be evaluated selectively, and if the data are found to be necessary, they should be collected and stored in the applicant's file and made available on request by means of the consultation procedure envisaged in Article 7 of the Proposal.

In case other instruments of the Schengen acquis required that such data be provided, such instrument should also be amended accordingly for the sake of coherence.

b) Grounds for refusal of the visa

The Working Party further draws attention to the inclusion of the items contained in Article 10.2.d) as grounds for refusal of the visa.

It is to be underlined that the existence of the grounds set out in letter d) may already have resulted into an alert on the applicant as referred to in letter c), pursuant to Article 96 of the Schengen Convention, and such alert may be accessed in full by visa authorities; therefore, this circumstance should be regulated by the said letter c).

Regarding the inclusion of "public health" among the standard grounds for refusal of a visa, it is to be pointed out that it is currently an innovation compared with the Schengen acquis – which is the foundations of the Proposal; as such, it is liable to the individual Member State's

discretion as for its application if it is not specified in greater detail. The Working Party requests that letter d) be deleted, or at least that the references to the possible threats be drafted more clearly and narrowly, adding specific references to EU wide definitions of the said concepts.

The amendment of the Common Consular Instructions via a new Regulation of the Parliament and the Council, which is envisaged by the proposal itself, could be a good opportunity for introducing the necessary adaptations and changes[15].

c) Links to other applications

Finally, the WP would like to draw attention to letter d), i.e. "links to other applications". Far from being related merely to the technical operation of the system, this feature might actually produce specific effects with regard to data subjects; therefore, it requires legal regulations to specify its scope and the attending safeguards. In particular, interlinking of information might allow users to access information to which they are not entitled. There should be safeguards in place to ensure that the interlinking does not change the existing access rights to the different categories of data in the VIS.

2.4. Specific problems: biometrics

Regarding the inclusion of biometric data into the system, Recital no. 9 only refers to the need "to ensure exact verification and identification of visa applicants" (both procedures being defined in Article 2, numbers 10 and 11). Article 3 refers to "photograph" (letter b) and "fingerprint data" (letter c).

The Proposal should be supplemented by adequate safeguards as applying to data that are especially sensitive, as already requested by the WP in its Opinion of 11.08.2004 (Opinion 7/2004). It is necessary to better 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, and whether alternative approaches that did not involve such risks had been or could be studied".

Assessment of the principle of proportionality in these questions of visas and free movement of persons inevitably, therefore, begs the question of the fundamental legitimacy of collecting these data and does not only concern the processing procedures (modes of access, storage period etc.)".

The utmost care should be taken when devising solutions that entailed inclusion of biometric information into the database; attention should also be drawn to the possible expansion of the access scope to include entities other than those that had been envisaged initially.

Special attention should be paid to the proportionality principles, in the light of a solution that would lead, over and above the legal checks prior to the issue of the documents in question and the inclusion of biometric data in them, to the storage in databases for the purpose of carrying out subsequent checks on illegal immigrants (particularly those without documents) of biometric data on all non-nationals applying for a visa or residence permit, when this data relates to traces that everyone leaves in their everyday life.

An extremely careful analysis of the lawfulness of processing such data for identification purposes is necessary, given the possible prejudicial effects to the persons concerned if they are lost or used for purposes other than those for which they were intended.

[15] See Recitals no. 6 and 8.

Account should be taken of the possible consequences in case identification data and fingerprints are matched erroneously when collecting the fingerprints data – which might be done on purpose if an individual whose digital fingerprints have been collected does not otherwise communicate his or her real identity. In those cases the hijacked identity would then be permanently associated with the digital fingerprints in question.

The circumstances under which the fingerprints are collected must guarantee perfect reliability.

The proposal should be supplemented by information on the "enrolment"-phase of the taking of fingerprints and on the mechanisms to be implemented by the visa authorities in collecting biometric data; in this regard, the WP asks for the inclusion in the Proposal of specific rules, aimed at ensuring a high level of reliability in the process of collecting and verifying the biometric data at this very moment, in particular to prevent the risk of identity theft.

Guarantees are also to be envisaged for those individuals who cannot provide some of the biometric data used, such as fingerprints (for example, if they have lost fingers, or their fingerprints have been damaged) in order to prevent them from being deprived - on this sole ground - of the opportunity to apply for and obtain a visa. Special attention must be paid to children and aged persons.

In addition, it might be appropriate to specify that the data should not be used in a manner that is incompatible with these purposes by laying down specific safeguards.

There have to be particularly rigorous checks if these biometric data are to be stored in a centralised database, as this would substantially increase the risk of the data being used in a manner that was disproportionate to or incompatible with the original purpose for which they were collected. [16]

Although the scope of these principles may be restricted in certain cases under Article 13 of Directive 95/46/EC, the relevant conditions for the establishment of such restrictions must obtain and the restrictions must derive from clear and precise legal provisions.

Multiple purposes can be legitimate only if the principles mentioned above have been specifically applied to each of them.

Reliability problems might arise from the creation of such a large database, both in terms of accesses and in terms of false-positive and/or false-negative findings – with potentially harmful consequences for the persons concerned.

Use of biometric data for identification purposes should be limited selectively; inclusion of these data in the CS-VIS should be envisaged where it is absolutely necessary – for instance in connection with suspected procedural misuse, or else in respect of an applicant whose data are already stored in the system and whose request has been rejected for serious reasons.

The availability of biometric data in the VIS should be limited to those specific cases in which the system already includes data on a given applicant, whilst they should only be exchanged in connection with cooperation activities involving the competent authorities (an issue that might be regulated in Article 7 rather than in Article 6).

"Fallback procedures" must be developed and included in the proposal in order to cope with the above problems by respecting human dignity without affecting the security level of the visa policy.

[16] See, in particular, the Working Document on Biometrics of August 2003 (WP 80) http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf.

Additionally, the technologies applied should lead to only a very low false-rejection rate, given the grave consequences for legitimate holders of documents.

Adequate guarantees should be laid down, particularly in the event of rejections in border checks, to ensure that the persons in question will be informed both of the reasons for the rejection and of the means by which they can assert their own point of view before any decision is taken (Article 15 of Directive 95/46/EC on automatic decisions), and that the facts will be clarified without delay.

As for the use of biometrics for verification purposes – an issue that is especially relevant with a view to applying Article 16 of the proposal – reference is made to point 2.6 below (Use of data for checks on visas).

2.5. Data subjects concerned

The WP would like to express its concerns about the provision envisaging the availability of personal data on several categories of data subject without any proof of a real need justifying it with relation to the purpose of the processing.

a) Data on third country nationals applying for a visa

Regarding short stay visas, the WP would like to draw attention to the status of third country nationals who are lawful residents in the territory of Member States. According to Article 21 of the Schengen Convention, a third country national holding a valid residence permit issued by one of the Contracting Parties may move freely for up to three months within the territories of the other Contracting Parties. [17] The text of the proposal should clarify this point, and the definition of "third country national" for the purposes of the Regulation should be amended to mean "any person who is not a citizen of or legally resident in the European Union…". If the current definition is kept, it should be made clear that the Regulation does not apply to third country nationals who are legally resident in the European Union. Accordingly, data on visa holders who have subsequently obtained a residence permit should be deleted when this happens.

b) Data on other members of the group

The definition of 'group member' contained in Article 2 of the proposal and the reference to "applicants travelling in a group" in Article 5.4 (providing for a link between applications) should be specified better as it might lead to considering as such even persons with fairly insignificant links with one another (clients, fellow nationals, colleagues…). The definition of 'group member' and the distinction to be drawn with regard to "group visas" should be clarified and based on precise, objective criteria.

[17] The Schengen acquis as referred to in Article 1(2) of Council Decision 1999/435/EC of 20 May 1999 (*), OJ L 176, 10.7.1999, p. 1.: Article 21:
"1. Aliens who hold valid residence permits issued by one of the Contracting Parties may, on the basis of that permit and a valid travel document, move freely for up to three months within the territories of the other Contracting Parties, provided that they fulfil the entry conditions referred to in Article 5(1)(a), (c) and (e) and are not on the national list of alerts of the Contracting Party concerned.
2. Paragraph 1 shall also apply to aliens who hold provisional residence permits issued by one of the Contracting Parties and travel documents issued by that Contracting Party immediately."

c) Data on persons issuing invitations

Article 6 of the proposal provides that the visa authority should enter "details of the person issuing an invitation or liable to pay the costs of living during the stay" in the application file. The Working Party notes that such categories of data may be relevant or necessary in case a precise enquiry is launched with regard to specific individuals and concrete violations of legal provisions. Their processing would be, however, excessive and disproportionate with regard to the routine implementation of the visa policy, which can be expected to require the sets of data listed under Article 6. Therefore, the Working Party calls for the deletion of this category of data or at least for it to be moved from Article 6 to Article 7 (categories of data to be entered into the VIS in case of consultation between central authorities), except where is a justified need.

2.6. Access to the VIS

The WP is confident that, pursuant to the commitments made by the Commission, it will be possible shortly to be provided with a complete, detailed picture having regard to the various initiatives currently undertaken by the Commission and the Council within the framework of Title IV of the TEC insofar as they entail the processing of personal data and/or exchanges of information. The principles of EC Directive 95/46 are fully applicable in this area and respect for Article 8 of the European Human Rights Convention is not a matter of self-certification.

Privacy, like security, should be considered in a horizontal manner. It should not be regarded as a hindrance to deployment of a given system, but rather as an asset. Addressing privacy/security after design specifications and design parameters have been laid down is likely to require re-designing elements of the system at a later stage, thereby leading to additional expense.

a) Centralised data and recipients

The authorities enabled to access the VIS, and the operations each authority is allowed to perform, are specified in the Proposal by having regard to the individual purposes sought.

Article 4 provides for publication of the list of the national authorities that will be able to access the data in the centralised database. The WP would recommend that the list be updated, preferably on a regular basis, in order to take account of supervening changes. The proposal would seem not to envisage any access to the VIS at EU level, even though supplementary information on the authorised departments/offices and the access levels respectively assigned should be made available to data protection authorities in order for them to be in a better position to discharge their supervisory and control duties.

b) Use of data by other authorities mentioned in Article 16 to 19 of the proposal

As for the provisions envisaging access to VIS by authorities other than those competent for the issuing of visas, reference should be made to the considerations made above on the need to ensure compliance with the purposes that correspond to the legal basis underlying the proposal.

Therefore, its use should be limited to the essential purposes inherent in the common visa policy, also in the light of the risk of errors and/or unauthorised access referred to above.

Other purposes that are more closely related to the protection of public security are pursued by other information systems within the EU – first and foremost the Schengen system, which will be joined by the VIS.

c) Use of data for checks on visas

"The competent authorities for carrying out checks at external border and within the territory of the Member State" may access the VIS for the purposes of "verifying the identity of the person" and/or "verifying the authenticity of the visa" (as per Article 16 of the Proposal).

Verification would consist in matching the data contained in a document submitted (passport and/or visa) with the person (document holder), i.e. – as specified in the Definitions – in the "process of comparison of sets of data to establish the validity of a claimed identity ".

In principle, it would not appear to be necessary for the purpose of verification to store the reference data in a database; it is sufficient to store the personal data in a decentralised way (e.g. by using a microchip), as pointed out by the WP in its working document on biometrics adopted on August 1, 2003[18].

Reference should also be made to the draft Regulation on a uniform visa model, which envisages a local storage medium (microchip) or other system allowing the claimed identity to be verified locally by means of a tool that is under the control of the person concerned. The WP continues to consider the latter system both preferable and considerably less privacy-intrusive.

It is appropriate to restrict access to the CS-VIS by only allowing it if verification is negative and it is necessary to identify the person in question. However, in the latter case the identification procedure should be carried out by suitably trained staff and over a longer time span than that usually available to perform standard border checks. Not all members of the checkpoint staff should be authorised to access the system, partly because the said staff can access the SIS data – in particular, the persons on whom alerts have been entered with a view to their non-admissibility – as well as the national information system.

The current wording of the draft Regulation should be improved in order to restrict the processing of personal data exclusively to the aforementioned purposes, in particular by specifying the authorities enabled to access the VIS online more precisely and selectively as well as by introducing functions to allow regularly monitoring accesses also via an internal audit system.

As for the verification procedure performed by competent authorities for carrying out checks "within the territory", it is suggested that the authority that is being referred to should be specified. Use of data for checks on visas is provided for in the draft Regulation as an additional "benefit" in pursuing the aim of the VIS, i.e. improving the common visa policy; therefore, the competent authorities could not but be the visa authorities referred to in number 3 of Article 2 – also by having regard to the circumstance that identity checks on a State's territory may be carried out by means of connections with SIS and/or other existing databases set up for police purposes.

[18] Document WP80 of 01.08.03, available at http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf.

d) Further access to VIS by authorities not included in the Commission proposal

The WP took note of the Conclusions adopted by the Council of 7 March 2005, whereby "access, for the purpose of consultation, should be guaranteed to Member States authorities responsible for internal security in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats".

Said access is to be allowed via an ad-hoc proposal based on Title VI of the TEU, which the Commission is required to submit "with a view to its adoption within the same time frame as of the Regulation on the VIS".

The purposes of data processing within the VIS should be, as stated before, the implementation of the visa policy. Access to VIS data should therefore be envisaged, as a matter of principle, only by public authorities in charge of implementing such policy, and the technical specifications should be designed accordingly to serve that purpose and to allow access to those authorities.

Access and use of VIS data by the authorities in charge of that fight must always be considered in the light of the purpose of the VIS and granted only to that end.

The envisaged expansion of the scope of access compared with the provisions made in the draft Regulation should be evaluated quite carefully by considering whether it is necessary in connection with the purposes set for the system.

Access by other authorities could only be legitimate on an ad hoc basis, in specific circumstances and subject to appropriate safeguards. Any rule allowing systematic or routine access would clearly go beyond what may be considered as a "necessary measure in a democratic society" and would not be deemed lawful.

Accordingly, the technical specifications for accessing the data in the VIS system should be designed in order to exclude such *routine* access by other authorities and for other purposes.

Even less should the system be technically shaped to allow certain types of access that would only be useful for those other purposes.

Data protection authorities must be properly involved in the discussions on the design of such technical specifications at an early stage.

The concept of "authorities responsible for internal security" should be clarified further in order to make clear the reference to authorities competent for law enforcement activities. (Third pillar authorities).

2.7. Interoperability of VIS and SIS II

The Working Party had already expressed its concerns in respect of the broad scope of the database under construction, including the possibility that its use might be enhanced further by having regard to the interoperability of European databases and/or the synergies between current and future information systems (SIS II, EURODAC).

Regarding the request made by the Council to the Commission to submit proposals for enhanced interoperability between European databases and to explore the creation of synergies between existing and future information systems (SIS II, VIS and EURODAC) in order to exploit their added value within their respective legal and technical frameworks in the prevention of and fight against terrorism, the need for ensuring compliance with the purposes for which the VIS is set up is re-affirmed by the WP, without prejudice to the assessment of the relevant legal basis.

It must be quite clear that the basic concept of the legitimate and proportionate collection of data from an individual and further processing of such data for a precise, legitimate, purpose (i.e. issuing a Schengen visa) should not leave room to the concept of a data base that can be shared by different authorities to pursue different purposes.

Interoperability should never lead to a situation where an authority, not entitled to access or use certain data, can obtain this data via another information system.

The Working Party reiterates its firm intention to contribute to shaping the way in which this interoperability will be configured in concrete.

Special importance is to be attached to ensuring an adequate public debate with the contribution of Member States' Parliaments and all other stakeholders concerning the impact of this initiative of individual rights.

The WP would also like to draw attention to the opinion on the development of the SIS II issued by the Schengen Joint Supervisory Authority[19] and is confident that the Commission will always timely brief the WP on the proposals being drafted, in order to allow it to provide its timely contribution - unlike what has been unfortunately the case with the draft Proposal on SIS II.

2.8. Data Retention

The Working Party welcomes the circumstance that the draft Regulation envisages a period of five years for keeping the data as a maximum. Similarly, it welcomes the addition of a specific provision (Article 22) which requires – pursuant to the purpose specification principle – deletion of data on persons who have obtained the nationality of a Member State, although this same provision should be applicable to aliens who lawfully stay in Member States (long-stay migrants).

More selective retention criteria should be defined, taking into account the different situations which may occur in practice and the different types of visa that may be issued.

For example, details where an individual has been detected making duplicate or fraudulent applications in other names may be retained for a longer time than those where travel documents were issued and travel undertaken without a problem. Furthermore, it seems disproportionate to keep for more than 2 years data on visas issued for less than 3 months, especially where the short-term visit has concluded without particular incidents.

A specific criterion may also be retained for frequent travellers when it may speed up the application process.

Such variety of situations should be taken into account by appropriately laying down different retention periods applied to the VIS, with particular regard to the provisions envisaging automatic linkage between an application and any other data contained in the system.

In any case, such differentiated retention periods should never exceed the general maximum of five years envisaged in the proposal. In particular, the WP suggests the following benchmarks:

- Data about persons where they have been refused a visa should not in principle be kept for longer than weeks or months, as deemed necessary to prevent visa shopping. This should

[19] Opinion on the development of the SIS II, http://escher.drt.garanteprivacy.it/garante/navig/schengen/home.htm.

be more the case when the reason is of an administrative nature, as in the cases provided for by Article 10.2. letters a) or b).

- In those cases where the visa has been refused for public health reasons, the data should be deleted as soon as that public health reason has disappeared.
- The retention period for data on a visa refusal based on a SIS alert should be made consistent with the maximum retention period for the SIS alert in the SIS itself. The general retention period in the SIS is 3 years for non-admissible foreigners. Keeping this SIS data for a longer period in the VIS would circumvent the provisions for data re-examination and deletion of the SIS. Therefore, data on visa refusals based on SIS alerts should be deleted no later than 3 years after the SIS alert has arisen.
- Biometric data must be kept in the VIS only under the circumstances referred to in paragraph 2.4.
- Links to other data related to group members must in principle not be retained after expiry of the issued visa.

2.9. Data subjects' rights

a) Information

The Proposal draft would appear to be adequate as for the right of information that is vested in data subjects – the latter including not only the visa applicant, but also the persons issuing an invitation as per Article 6(4), letter f).

However, with regard to visa applicants, Article 30(1) should be supplemented by providing for the obligation to inform on the following items:

- period of data retention in the VIS;
- mechanisms to exercise access and rectification rights in respect of the data controller (i.e. the authority competent in each contracting Party for entering the data in the VIS);
- name and contact details of the national supervisory authority the applicant may apply to if he/she is not satisfied with the reply.

Additionally, paragraph 2 of the said Article should specify more clearly that the data controller should provide the information set out in Article 30 at the time of data collection - by means of the relevant designated agent(s) at consulates and diplomatic representations – adding, as far as biometric data are concerned, further information concerning the data stored on an electronic medium, in particular the data that cannot be read directly on the surface of the document.

b) Access to one's own data

The wording of Article 31 should be clarified in order to make clear that the right of access may be exercised by the data subject, by directly applying to the competent authorities in Member States who are the data controllers.

To that end the meaning of "competent authorities" should be clarified (data controllers).

The data subject should be properly informed no later than the moment of collection of the data about the authority acting as the data controller, and how to exercise his rights of access, rectification and deletion directly with this authority.

It should be specified in the text that there is no access to the CS-VIS, because CS-VIS is only processing data on behalf of each Member State; therefore, data subjects may claim their rights by applying to the competent authority of the Member State responsible for entering the relevant data in the VIS.

Paragraph 6 should be supplemented by referring to the possibility for a data subject to apply to the respective national data protection authority if his/her application is rejected, or if the reply provided by the competent authority is found not to be satisfactory.

Articles 32 and 33 should be improved as to the reference to the role played by national data protection authorities. If a data subject can directly access his/her data and exercises this right by means of an ad-hoc application/request to the data controller as per Article 31, the data protection authority is in charge of the tasks set out in the national legislation transposing Directive 95/46/CE in this respect; this circumstance should be reflected in the wording of both Articles.

In particular, both the title and the first paragraph of Article 32 refer to cooperation among the competent authorities, whilst the other two paragraphs are addressed to data protection authorities as the authorities in charge of supervising and verifying lawfulness of the processing.

c) Correction

The data subject's right to have incorrect data deleted is provided for in the draft, however "data recorded unlawfully **may** be deleted" (paragraph 2 of Article 31). The WP would like to see the word "may" replaced by "must", as it conflicts with the principles set forth in Article 6 of the Directive and is not in line with the provisions made in paragraph 4 of Article 31 either.

2.10. Security

The draft Regulation contains specific provisions about the risks that processing involves and the nature of the data to be protected. The WP reiterates the importance of proper security measures and recommends in particular that :

- Measures should be introduced to allow systematic monitoring of and reporting on the effectiveness of the security measures, in particular those set out in Articles 25 and 26;
- To that end, the monitoring and evaluation tasks entrusted to the Commission should be extended to all aspects related to lawfulness of the processing as well;
- Precise user profiles and the complete list of user identities should be created and made available, in particular to national data protection authorities;
- In addition to the recording of all data processing operations, regular self-auditing procedures should be envisaged for the VIS. The relevant reports should be made available to data protection authorities in order to facilitate auditing by focusing on major criticalities;
- The data intended for transmission under the VIS system should be encrypted so that they cannot be accessible to unauthorised third parties;
- Functions should be envisaged to ensure immediate recovery in case of interruption of the systems as well as that stored data cannot be corrupted because of a malfunctioning of the system.

The WP would also like to see specific information on the security measures to be adopted by visa authorities in order to ensure accurate identification of the person whose biometric data are enrolled and subsequently coupled with census data, as well as concerning the obligation of the aforementioned authorities to inform data subjects and ensure that :

- The data cannot be modified by an authority other than the one responsible for issuing the document in accordance with ICAO Recommendation 9303, as referred to in Recital 2 (electronic signature certified by the ICAO); and
- The data contained in the microchip on the issued document cannot be accessed without the persons concerned being aware of it. Neither should they be accessed by public bodies other than those legally authorised or by private entities.

In this regard, the WP pointed out in its Opinion no. 7/2004 that it would be appropriate to provide for encryption of the data in order to ensure confidentiality, and that access for reading the electronic elements could also be protected by an individual code known only to the holder.

2.11. Responsibility for the System and Independent Supervision

a) Responsibility for the system (Member States/Commission)

Article 23 (2) of the draft Regulation provides that the data shall be "processed by the VIS on behalf of the Member States" and Article 23 (3) that the Member States shall designate the authority considered as controller in accordance with Article 2(d) of Directive 95/46/EC.

The Commission is responsible for the central portion of the VIS (CS-VIS) as well as for national interfaces; Member States are responsible for national systems. The data are entered by the competent authorities of Member States, and only those authorities may modify the data pursuant to Article 21 of the Proposal.

Each Member State is to be considered a controller, in the meaning of the Directive.

The role of the Commission is not as clear. As a result, the role of the Commission as a controller and/or processor deserves future attention.

The Working Party therefore stresses that the fact that the Member States have some responsibilities as to the functioning of the system does not exclude that the Commission would also be responsible for some aspects, as a co-controller.

The WP would like to be provided with a more specific description of the role played by the Commission with regard to the VIS, in order to understand who and how is responsible for the lawfulness of the processing of data in the VIS and allow the national data protection authorities and the European Data Protection Supervisor (EDPS) to play their supervisory roles and better coordinate their respective activities – so as to prevent gaps in monitoring operation of the system.

b) Supervision

The supervisory task is shared between national supervisory authorities, as for the national system linked to the national interface, and the EDPS as for the features falling under the Commission's responsibility.

Regarding the coordination between national data protection authorities and the EDPS, a more specific decision on this matter may only be made once the requested clarification on the role played by the Commission is obtained.

c) Implementation

In the WP's view, there is not enough information about the various ongoing initiatives, the studies and the activities in progress.

There are several sensitive issues that should not be decided upon exclusively by means of a comitology procedure – in the light of their impact of fundamental rights including the protection of personal data as well as in the absence of the clarification requested.

Therefore, the ultimate decision on all issues liable to impact on fundamental rights and personal data protection should be left to an instrument of primary legislation, which can better ensure careful assessment of the proportionality of the measures in question.

The comitology procedure might be helpful to specify the technical arrangements to implement the legal approaches determined in the manner described above.

3. Conclusions

The VIS Regulation is intended as an important component of the area of freedom, security, and justice.

The Commission Proposal contains rather complex considerations and requires an articulated, in-depth analysis, which the Working Party has outlined in the preceding sections.

The Working Party recalls with satisfaction that, on the occasion of the speech addressed by the Commission's Vice-President to data protection authorities on 21 December 2004 and 18 January 2005, the commitment was made towards enhanced cooperation with data protection authorities in order to bring about a new generation data protection by having regard to the establishment of new databases, new information exchanges, and new forms of police and judicial cooperation.

On that occasion, the Commission also highlighted the need for a consistent action plan and drew attention to the proportionality principle and the impact produced on fundamental rights by the new regulatory initiatives, whereby the involvement of data protection authorities was to be regarded as an added value to be pursued.

Based on these premises, the Working Party would like to express its thanks for the attention it has been paid; it takes note of the requirement that the initial efforts made via the draft Regulation be supplemented by definite improvements in the text, resulting, firstly, into a more systematic overview of all the law-making work in progress on similar initiatives and related measures, and secondly, into clarifying the implications related to the complex architecture of an information system that is expected to contain data on several tens of millions of individuals.

The Working Party re-affirms that it is ready to give its timely contribution to the passing of legislation in which data subjects' fundamental rights and the public interests at stake can be reconciled in a balanced manner, also by means of other opinions the Commission will

hopefully request from it as well as via such other cooperation mechanisms as may be deemed useful.

Within this framework, the Working Party would like to see the text of the Proposal amended in the light of the following remarks:

1. The Working Party underlines that the structure of the VIS as envisaged in the Proposal implies massive collection and processing of personal data with far-reaching consequences on the individuals fundamental rights, in particular their right to privacy. It is of the utmost importance that such processing complies with the principles contained in the European Convention on Human Rights, the European Charter of Fundamental Rights, Council of Europe Convention No. 108, and more specifically, Directive 95/46/EC.
2. A strict observance of the principles of necessity and proportionality should be guaranteed.
3. The purpose of the collection and processing of personal data in the VIS should be closely defined and limited to the need for improving the Common Visa Policy, in line with the legal basis of the Proposal.
4. Only those categories of data essential to that purpose should be processed, and categories of data that may produce discriminatory effects such as, for instance, the applicant's nationality at birth should be excluded.
5. The standardisation of the "grounds for refusal of the visa" or the use of "links to other applications" should be subject to the condition of the categories of data being clearly defined so as to limit discretion in the exercise of public authority.
6. Concerning certain categories of data subjects, the VIS should not contain data on third country nationals holding a valid permit or subsequently obtaining it, whilst "other group members" should only be included on the basis of a precise and clear definition of "group member"; data on "persons issuing invitations" should not be available for routine implementation of visa policy, and be limited to precise enquiries for concrete violation of legal provisions.
7. The Working Party welcomes the circumstance that the draft Regulation envisages a maximum period of five years for keeping the data. Nevertheless, more selective retention criteria should be set out in the Proposal, taking into account the different situations that may occur in practice, the different types of visa that may be issued, and the different grounds for refusing a visa.
8. The processing of biometric data imposes that additional safeguards are put in place; in particular:
    a. The collection of biometric data should be carried out in a way that ensures a high level of reliability, in particular to prevent identity theft.
    b. Storage in a centralised database should be extremely limited and at any rate subject to particularly stringent checks.
    c. Use for identification purposes should be limited to cases where it is absolutely necessary, i.e. in case of procedural misuse following previous visa rejection. It should be conducted in a way that guarantees very low false-rejection rates, and adequate safeguards should be put in place in the event of a rejection

(information on the reasons and means to have the automatic rejection reviewed in a non-automatic way).

9. Access to the data must be limited to identified authorities and take place under circumstances that are consistent with the purpose of the system. Only authorities in charge of implementation of visa policy may have routine access to the VIS. Other authorities, in particular law enforcement authorities, should only be able to access the data on a case by case basis, under specific circumstances connected with a particular enquiry, and subject to appropriate safeguards. The technical features of the system, including interoperability, should be designed to guarantee that these limits are respected, with particular regard to the envisaged links with the SIS.
10. The role played by the Commission with regard to the VIS should be specified better, in particular to allow the national DPAs and the EDPS to play their supervisory roles and coordinate their respective activities.
11. The provisions on the implementing role played by the Commission under comitology rules (Article 39) should be re-drafted to specify that they only apply to issues that do not impact on fundamental rights and the protection of personal data.

Done in Brussels, on 23 June 2005

For the Working Party
The Chairman
Peter Schaar