

**Comments Standing Committee of experts in international immigration, refugee and criminal law
on the draft proposal for a Regulation concerning the Visa Information System (VIS),
COM (2004) 835**

Utrecht, April 2005

1 Introduction

The Standing Committee repeats its general concerns with regard to the establishment of the Visa Information System (VIS) as expressed during the consultation procedure.¹ According to the Standing Committee the present proposal for a Regulation on VIS should not be adopted on the following grounds:

- The necessity of a new large scale database with a risk and an extensive impact on privacy and human rights of individuals has not been justified.
- Before the establishment of VIS, Member States should adopt clearly harmonized rules on procedures for visa applications by revising first the Common Consular Instructions (CCI).
- The actual decision-making with regard to VIS lacks democratic accountability.
- The draft proposal of the Commission includes only a partial regulation of the future functioning of VIS. Important issues on the future use and impact of VIS have not been provided for in this proposal. Therefore, a complete and transparent assessment of the value or effects of VIS cannot be made by the European Parliament nor by the national parliaments.
- The proposal does not provide for a legal framework with regard to the powers of national authorities, the consequences of a VIS registration for the legal position of the persons concerned, nor the possible access by other authorities to VIS.
- The role given to (EU and national) data protection authorities, neglects their difficult and overburdened position. At this moment these organizations lack sufficient financial means and powers to protect effectively the rights of the individuals concerned. The VIS Regulation should only be adopted after sufficient means and effective control powers to control the use of VIS have been granted to the data protection authorities.
- The present proposal does not provide for effective legal protection for the individuals whose information will be stored into VIS.

2 Balancing the need for VIS: principal objections

Added value has not been established

VIS will include data on millions and millions of visa applicants and on the EU nationals and long term resident third country nationals who invite these persons. According to the proposal, each record on a visa application will be stored for five years and this record will include biometrical data on the applicant. This database is to be used on a large scale by at least 25 countries. This implies that any incorrect data which has been entered by an authority of one the EU Member States will thus have large-scale and long-term effects for the person concerned. The large scale of this system enlarges as well the risk of unauthorized access to this system. This new measure will not only have intrusive effects for individuals, but also high financial costs for Member States. A very clear and convincing motivation of the necessity of this measure is therefore required. We refer to the new principle, incorporated in The Hague Program², according to which each new centralized European database should be created only on the basis of studies that have shown their added value. As has been laid down in a previous decision of the Council, VIS is to be used for different goals, such as the implementation of the EU visa policy, the fight against

¹ See our letter of 12 May 2004, CM0409.

² 13302/2/04, p. 22, see section 2.1.

terrorism, readmission policy, and the implementation of the Dublin II regulation (on the assessment of the responsibility of Member States for asylum applications).³ This multiple use of VIS makes a complete and appropriate cost-benefit analysis of the establishment of VIS a very difficult, if not impossible task. According to the Standing Committee, the Extended Impact Assessment, which has been presented together with the draft Regulation on VIS, does not establish the added value of VIS for each of the different goals pursued.⁴ This report only describes four alternative options for the exchange of visa data: 1. No VIS; 2. Entry-Exit system; 3. VIS without the use of biometrics; and 4. VIS with biometrics. Each option is assessed on different merits, for example the impacts for the efficiency of a common visa policy and border checks, its contribution to internal security, its financial costs, and the impact on fundamental rights, in particular the protection of personal data and privacy. When considering, option 1, 'No VIS', the report treats marginally the possible other solutions by which the envisaged goals could be reached. With regard to the effects of option 4, the use of VIS with biometrics, for tracking terrorists or organized criminals, the impact assessment report even concludes that this would only be limited and dependent upon the effectiveness of other measures taken.

Use of biometrics: extended risk

With regard to the choice of integrating VIS with biometric identifiers, the Extended Impact Assessment report underlines the risk and the extensive impact on privacy and human rights. On p. 45 of the report it is stated:

'If there would be no appropriate safeguards on data security in place, personal data entered and processed in VIS with biometrics could be open to unauthorized access and alterations either by authorities not authorized to do so, or by criminals who would be eager to steal the identity of legitimate travelers or correct the record of their own personal data.'

Data protection authorities expressed their concerns on the use and central storage of biometrics. On 21 December 2004, the French Data Protection Authority, CNIL published a report on the proposals of the French government to register biometric data of those aliens whose visa had been refused.⁵ CNIL considered this national measure neither justified nor necessary. According to CNIL, this measure would entail the risk of stigmatisation of those persons being refused a visa, and, as being entered into this new system, would be refused a renewed application for a visa. Previously, the Article 29 Group also advised against the establishment of a centralized registration of biometric data.⁶ There is no indication that the Commission has taken into account these positions.

Finally, it is important to keep in mind the technical imperfection of biometrics, as underlined by the European Data Protection Supervisor (EDPS).⁷ In the first place, 5 % of individuals are estimated not to be able to enroll because of having no readable fingerprints or no fingerprints at all. This would mean with regard to the use of VIS, which is expected to include data on 20 million applicants in 2007, that 1 million persons cannot be checked by the normal procedure. Secondly, with regard to biometrics, an error rate of 0.5 to 1 % is considered normal, which would mean a False Rejection Rate of 0.5 to 1 % with regard to measures and checks based on VIS. According to the Standing Committee, the consequences of such an error rate with regard to the use of VIS are not acceptable.

Direct and indirect discriminatory effects of VIS

VIS, if established, will in the first place affect the position and rights of third country nationals applying for a visa. The collection and the centralised storage of biometrical data of this group of persons is an interference with their right to private life as protected in Article 8 ECHR. The Standing Committee questions whether this difference of treatment has an objective and reasonable justification in the light of the non discrimination principle as laid down in Article 14 ECHR. According to case law of the European Court for Human Rights (ECtHR), a difference of treatment based exclusively on the ground of nationality, is to be considered discriminatory for the purposes of Article 14 ECHR, if there is no reasonable relationship between the means employed and the aims sought to be realised.⁸ As we argued above, VIS lacks this 'reasonable relationship'.

Secondly, the Standing Committee is concerned about the possible indirect discriminatory effects of VIS on the grounds of race and ethnic origin against EU citizens and lawfully resident third country nationals

³ Council Conclusions 19 February 2004, doc. 5831/04.

⁴ EPEC Final Report, December 2004.

⁵ See *L'expérimentation de visas biométrique: la position de CNIL*, 21/12/2004, on www.cnil.fr, visited in December 2004.

⁶ Working Document on biometrics of 1 August 2003, No. 12168/02/NL WP 80.

⁷ Opinion of the European Data Protection Supervisor on VIS, Brussels, 23 March 2005.

⁸ *Gaygusuz v. Austria* [1996] Reports 1996-IV para. 42.

in Member States, issuing an invitation or liable to pay the costs of living during the stay of the visa applicants. The majority of visa nationals are from African and Asian countries and their relatives and friends in the EU issuing them with invitations will be those persons entered into VIS on the basis of Article 6(4)(f) of the draft proposal. The explanatory memorandum (p.33) states that *'the inclusion of data on persons and companies issuing invitations will help to identify those persons and companies which make fraudulent invitations...(which) constitutes important information in the fight against visa fraud, illegal immigration, human trafficking and the related criminal organisations which often operate on an international scale'*. Given this purpose and the apparent intention of Member States to provide wider access to VIS to law enforcement authorities as well as the future consequences of interoperability, these persons, are likely to be disadvantaged disproportionately by the inclusion of their names and addresses in VIS, particularly in the event of any abuse regarding access to or use of this data.

3 Democratic deficit

The Standing Committee disagrees with the present decision making procedure on VIS, in which the European Parliament and the national parliaments are left with a very marginal role. Although the European Parliament has co-decisive right with regard to this proposal of a Regulation for VIS, the decision for the set up of VIS has factually been made in the decision 2004/512/EC of the Council of 8 June 2004 with regard to the legal basis of VIS.⁹ This draft decision was rejected by the European Parliament on 22 April 2004, however this (non binding) advise has not been taken into account by the Council or the Commission.¹⁰ Political decisions on the purpose and the future functions of VIS are already taken with the adoption of the guidelines on VIS by the Council in its meeting of 19 February 2004. During its meeting of 7 March 2005, the Council decided that national law enforcement authorities should be given access to VIS.¹¹ The European Parliament was never consulted on these guidelines, nor on the latter decision. Finally, without awaiting the final adoption of actual proposal on the content of VIS, IT companies have already been commissioned to build the architecture for VIS.¹² Important decisions on VIS and its final functions are thus solely made by the Council and the Commission, leaving no space for a real public debate and depriving the European Parliament from an effective legislative power.

4 Actual proposal is an incomplete regulation of the future use of VIS

The present proposal of the Commission includes only a partial regulation of the future functioning of VIS. Important issues on the use and impact of VIS have not been provided for in this proposal, which means that a complete and transparent assessment of the value or consequences of VIS cannot be made. The draft regulation does not provide for a legal framework with regard to the powers of national authorities, the consequences of a VIS registration for the legal position of the persons concerned, or the access by other authorities to VIS.

Competences of authorities based on VIS information

One of the purposes of VIS as presented by the Commission would be the prevention of visa shopping. It is however not clear in what way VIS actually will be used for this goal: will national visa authorities have the power to refuse a visa whenever they retrieve from VIS, that the visa applicant has been refused a visa by the Member States? In other words, is the effect of VIS that if a person has been refused a visa by one country, he or she will also be refused automatically a visa from the other participating countries? This would be a very far reaching consequence of the use of VIS, which should have been dealt with more explicitly by the Commission. It is noteworthy that the Extended Impact Assessment of VIS refers to *'the potential extremely grave consequences of the use of VIS for a traveler, resulting in a rejection of a visa application or refusal of entry into the territory of Schengen States'* (p. 46). This possibility of negative decision making, solely on the basis of a previous VIS registration, would run encounter the general principle of the EC Directive 95/46, Article 15, according to which a decision implying legal effects to a person, should not be solely based on automated data processing.

- The Standing Committee underlines that any regulation on the establishment and use of a European database such as VIS should provide for a clear prohibition of decision making solely based on information stored into that database.

⁹ OJ L 213/5, 15 June 2004.

¹⁰ Legislative resolution of the European Parliament T5 – 0352/2004.

¹¹ Conclusions meeting Council Competitiveness, 7.III.2005, doc. 6811/05.

¹² Commission Staff Working Paper on the development of VIS, 4 March 2005, SEC (2005) 339.

Interoperability VIS with other data bases

The European Council, in its Declaration on combating terrorism of 25 March 2004, invited the Commission to submit proposals for enhanced interoperability between SIS II, VIS, Eurodac and the use of this information for the fight and prevention of terrorism. A Communication by the Commission on this issue has not been published yet.

- According to the Standing Committee, decisions on the interoperability of VIS with other databases, should be dealt with simultaneously with the present proposal on VIS. The effects and consequences of VIS will depend on which links will be made with other databases. This use of VIS should be regulated in the present proposal for a Regulation, allowing a comprehensive and transparent decision making.

VIS and access by other authorities

During its meeting of 7 March 2005, the Council adopted the decision that *'in order to achieve fully the aim of improving internal security and the fight against terrorism,'* Member State authorities responsible for internal security should be guaranteed access to VIS, *'in the course of their duties in relation to the prevention, detection and investigation of criminal offences, including terrorist acts and threats.'*¹³

- This issue (access to VIS by police or security authorities) should have been dealt with more explicitly by the Commission in the draft regulation. If the latter issue is to be regulated in a third pillar instrument, this not only undermines the democratic accountability of the decision making, but also obscures the actual understanding of the meaning and consequences of VIS.

5 Data protection authorities lack sufficient means to monitor VIS

According to Article 35 of the draft Regulation, the European Data Protection Supervisor should monitor *'the activities of the Commission to ensure that the rights of persons covered by this Regulation are not violated by the processing of data in the VIS'*. National supervisory authorities are tasked in Article 34 of the draft regulation to monitor the lawfulness of the processing of the personal data in VIS by the Member State in question.

These new monitoring tasks which are given to the European and national data protection authorities do not take into account the actual lack of personal and financial powers for these organizations to perform their tasks effectively. Both at the European level as on the national level, these organizations have to monitor a wide range of developments with regard to data processing and the protection of human rights.

- The Standing Committee underlines that the (European and national) data protection authorities will have to be provided first with effective powers and sufficient financial means, before establishing new databases which they would have to monitor. The VIS Regulation should only be adopted after sufficient means and effective control powers to control the use of VIS have been granted to the data protection authorities.

6 Lack of legal protection for individuals

The Standing Committee is very concerned about the lack of legal protection of individuals with regard to decisions based on data bases such as VIS. The proposal includes an elaborated set of data protection rules, however does not include provisions offering the data subject the necessary additional protection at the level of immigration procedural law. For example, as mentioned above, the draft provides for the right of access to courts with regard to the rights on access and correction, but not with regard to the decisions which could be based on VIS, namely: refusal of a visa, refusal of entry, or the decision to transfer a person to a state which is to be considered as the responsible country to treat the asylum application of the person concerned (Dublin II). What is for example the legal position of third-country nationals who apply for a visa and then withdraw their application? In this light, it is important to highlight the conclusion in the Extended Impact Assessment report with regard to the protection of human rights and privacy: the *'extreme negative impacts ... would be mitigated if the person concerned were to be provided with precise information on the grounds for taking such a decision'*.

- The Standing Committee recommends that the rules with regard to the rights and legal protection of visa applicants should be harmonised first. The most appropriate place for the provision of clear and effective legal remedies to third-country nationals refused a visa would be in the

¹³ Conclusions meeting Council Competitiveness 7.III.2005, doc. 6811/05.

Regulation revising the Common Consular Instructions (CCI). The CCI should be revised first (and not just recast) to provide for clearly harmonized rules that should facilitate movement into the EU for visa nationals and safeguard their rights.

- Further, we propose to include the guarantees we have drafted in our earlier Directive on minimum guarantees for individual freedom, security and justice in relation to decisions regarding movement of persons, in any future regulation with regard to border control and visa applications.¹⁴

Article 3:

1. *Any decision as referred to in Article 1^{*}, affecting any person within the jurisdiction of a Member State or the European Community [European Union], shall be prescribed by law and shall be in writing with the indication of the legal provision or provisions underlying the decision and all relevant reasons. The person affected shall be informed in writing about legal procedures in order to have such a decision reviewed by a court of law, in accordance with Article 6 of this Directive. The decision shall indicate the competent court and its address.*
2. *Everyone within the jurisdiction of a Member State or the European Community [European Union], affected by any decision as referred to in Article 1, has the right to be informed of this decision without delay, either in person or by representative.*
3. *A decision on grounds of public policy or national security shall only be permitted if the measure is justified while the personal conduct of the person concerned indicates a specific risk of an actual and serious prejudice to the requirements of public policy or national security of one or more Member States.*
4. *Decisions as referred to in the first paragraph must be justified by overriding reasons based on the general interest; they must be suitable for securing the attainment of the objective which they pursue; and they must not go beyond what is necessary in order to attain that objective.*

Article 6:

1. *Everyone within the jurisdiction of a Member State or the European Community [European Union] has the right to an effective legal remedy before a court against any decision as referred to in Article 1^{*}.*
2. *This remedy must be easily and promptly accessible and offer adversarial proceedings before an independent and impartial court competent to review on the merits the reasons for the decision and relevant evidence, if need be with appropriate procedural limitations on the use of classified information. The court will decide within a reasonable time. The court will decide speedily when detention is at issue or when personal liberty and integrity are affected in any other way.*
3. *Proceedings must offer the individual concerned the opportunity to be heard either in person or by representative. The principle of equality of arms must be abided.*
4. *The court must have the power to order effective suspension of the execution of measures whose effects are potentially irreversible for the period of the proceedings.*
5. *The court must have the power to annul a decision when it finds the decision arbitrary, disproportionate or unlawful.*
6. *The court must be competent to order any appropriate measure against the responsible authority of any Member State repairing or compensating damages caused by such decisions.*

7 Remarks with regard to specific provisions of the draft Regulation

Links with other files or databases

Article 3, describing the categories of data entered into VIS, includes in 3.1 (d): '*links to other applications*'. This provision has not been explained at all in the explanatory memorandum of the draft regulation. If this is to be interpreted broadly, it allows Member States to add or connect to the VIS files

¹⁴ P. Boeles a.o., Border Control and Movement of Persons, Towards effective legal remedies for individuals in Europe, Utrecht 2003 (Meijers Committee).

* Article 1 of our proposal refers to decisions concerning refusal of entry or residence or refusal to issue a visa or residence permit; refusal of permission to board, or to disembark from carriers; detention or limitation of his liberty to move, for purposes of immigration control; expulsion, removal, deportation and listing for the purpose of refusal of entry; and, processing of personal data including biometrical and DNA information.

any application, data file or personal data they like. Also this could mean that VIS would be linked to other EU databases such as Eurodac, SIS II or Europol. This should have been dealt with explicitly in this regulation, to allow a political debate on this fundamental issue.

- If this provision is to be interpreted in connection with Article 5 of the draft Regulation and only refers to the previous applications of the individual applicant stored into VIS, this should be explicitly made clear in the regulation by amending Article 3.1(d) either by deleting (d) or by adding ‘..., as meant in Article 5’.

Access by other authorities

Article 16 of the present proposal regulates the use of data for checks on visas by ‘*competent authorities for carrying out checks at external borders and within the territory of the Member State*’ without defining these authorities.

- The access by other authorities to VIS should be regulated more explicitly by making it clear which authorities have access to VIS for which tasks.

Right to information

With regard to the right of information in Article 31: this does not provide for a time limit within which the authorities would have to inform a person on the information stored into VIS. Article 31 (2) only provides that the correction or the deletion of the data should be carried out ‘without delay’, and Article 31 (5) states that the refusal to correct or delete the data, should be explained in writing to the person concerned ‘without delay’. However these provisions do not apply to the communication of data recorded on the person concerned in the VIS.

- We therefore propose to add to Article 31 (1) ‘... *any person shall have the right to obtain communication within one month of the request by the person concerned of the data relating to him...*’

Responsibility for the accuracy and legitimacy

With regard to the responsibility for the accuracy and legitimacy of the data stored into VIS: the draft Regulation (Article 25) seems to include a ‘gap’ of responsibility: Member States are responsible for the lawfulness of the collection and transmission of the data in VIS, and for the accuracy and whether the data are up-to-date only ‘when it is transmitted to VIS’. This appears to mean that after the data have been transmitted to VIS, the Member States are no longer responsible. According to Article 25 (2), the Commission should only ensure that VIS is operated in accordance with the Regulation and implementing rules and in particular should ensure the security of the CVIS and to prevent unauthorized access to data processed in VIS. This does not include any responsibility for the lawfulness or correctness of the data once they are kept into VIS.

- The Commission, or the Member State which forwarded the data, should be made explicitly responsible for the lawfulness of the storage of the VIS data, and for the data being accurate and up-to-date, as long these data is kept into VIS.

Penalties on infringements of data protection law

Article 29 of the draft Regulation provides for the possibility for the Member States to lay down rules on penalties applicable on infringements of data protection provisions in this Regulation. These penalties should be ‘*effective, proportionate, and dissuasive*’.

- These penalties should have been provided for in this Regulation itself, at least the Regulation should have provided for minimum norms on these penalties. Also the Regulation should include a possibility for courts to order authorities to repair or compensate the damage caused by such decisions.