# EUROPEAN DATA PROTECTION SUPERVISOR

## Opinion of the European Data Protection Supervisor on the Proposal for a Regulation of the European Parliament and the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications (COM (2006) 269 final) — 2006/0088 (COD)

(2006/C 321/14)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28 (2) of Regulation (EC) No 45/2001 received on 19 June 2006 from the Commission;

HAS ADOPTED THE FOLLOWING OPINION:

### 1. **INTRODUCTION**

The proposed Regulation has two main objectives, both in view of the implementation of the Visa Information System:

— to provide a legal basis for Member States to take mandatory biometrics identifiers from visa applicants;

— to provide a legal framework for the organisation of Member States consular offices, especially by organising possible cooperation between the Member States for the processing of visa applications.

These two objectives raise different questions in terms of data protection and will be dealt with in distinct paragraphs, even though they form part of the same proposal.

The present proposal aims at amending the Common Consular Instructions (CCI). These were adopted by the Executive Committee established by the Convention applying the Schengen Agreement of 14 June 1985. As a part of the Schengen Acquis, they were inserted into EU law by a Protocol annexed to the Treaty of Amsterdam, and have been amended on several occasions since. Although a number of amendments remain confidential, the CCI were published in 2000. As to content, they are essentially a handbook containing practical rules on how to issue short-stay visas. They contain provisions on the examination of applications, the decision-making procedure, on how to fill in visa-stickers, etc.

## 2. COLLECTION OF BIOMETRIC IDENTIFIERS

### 2.1. Preliminary remark: specificity of biometric data

According to the VIS proposal ([1]) presented by the Commission on 28 December 2004, Member States shall introduce fingerprints and photographs as biometric identifiers in the VIS for verification and (or) identification purposes. The present Proposal for a Regulation of the European Parliament and the Council amending the CCI aims at providing a legal basis for the collection of biometric identifiers.

The EDPS issued an opinion on 23 March 2005 concerning the VIS proposal ([2]). In this opinion, he underlined the importance of surrounding the processing of biometric data with all the necessary safeguards, in view of their specific characteristics ([3]):

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

According to the EDPS, this sensitive nature of biometric data requires that the introduction of obligations to use these data should only take place after a thorough assessment of its risks and should follow a procedure allowing full democratic control. These remarks underlie the examination by the EDPS of the present proposal.

### 2.2. Context of the proposal

The context in which this proposal is made makes it even more sensitive. The proposed regulation cannot be seen in isolation from the development of other large-scale IT systems and the general tendency towards greater interoperability between information systems. This is mentioned in the Commission's Communication of 24 November 2005 on improved effectiveness, enhanced interoperability and synergies among European databases in the area of Justice and Home Affairs ([4]).

Therefore, a decision made in a given context and in view of a given purpose is likely to have an influence on the development and use of other systems built for other purposes. In particular, biometric data — probably including data collected for the implementation of the visa policy — could be used in different contexts once they are available. This could concern not only the framework of the SIS, but in all likelihood Europol and FRONTEX as well.

### 2.3. Obligation to provide fingerprints

The explanatory Memorandum of the present proposal states: 'As the taking of biometric identifiers will now be part of the visa application procedure, the Common Consular Instructions have to be amended in order to create the legal basis for this measure'.

The EDPS objects to the choice of the legislator to include provisions on whether or not to exempt certain individuals or groups of individuals from the obligation to provide fingerprints in the CCI, rather than in the VIS Regulation itself. Firstly, these provisions have a significant impact on the privacy of a great number of individuals and should be dealt with in the context of basic legislation rather than in instructions with a largely technical character. Secondly, the clarity of the legal regime would make it preferable to deal with this in the same text as the one establishing the information system itself.

---

([1]) 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) presented by the Commission on 28 December 2004

([2]) Opinion of 23 March 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, OJ C 181, 23.7.2005, p. 13.

([3]) *'[Biometrics] offer a quasi-absolute distinctiveness, i.e. each individual possesses unique biometrics. They almost never change throughout a person's life which provides permanency to these characteristics. Everybody have the same physical "elements" which also gives to biometrics a dimension of universality.'*, ibid.

([4]) COM (2005) 597 final.

(a) First of all, creating a legal basis for the mandatory fingerprinting and taking of biometric identifiers is much more than a technicality; it has a significant impact on the privacy of the individuals concerned. In particular the choice of minimum and/or maximum ages for fingerprinting is a political decision and not only a technical one. Therefore, the EDPS recommends dealing with this matter, and especially with the aspects which are not purely technical in the basic text (VIS proposal) instead of in a handbook of instructions on mainly technical and practical aspects of the visa procedure ([1]).

In this regard, it is also useful to recall the requirements of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and its case law. According to Article 8 (2) ECHR, any interference by a public authority with the exercise of the right to privacy is only allowed, if it is 'in accordance with the law' and is 'necessary in a democratic society' for the protection of important interests. In the case law of the European Court of Human Rights, these conditions have led to additional requirements as to the quality of the legal basis for interference (it must be provided for in an accessible legislation and be foreseeable), the proportionality of any measure, and the need for appropriate safeguards against abuse.

Apart from the fact that the piecemeal approach to legislation described here under does not make for clear and accessible regulation, one can wonder whether the CCI themselves can even qualify as such. There could be some questions surrounding the procedure for (possible) future amendment of this text. It should in any case be guaranteed that a decision of this importance cannot be amended without a procedure providing the appropriate transparency and democratic consultation.

(b) The second issue is one of clarity of the legal regime. The Explanatory Memorandum of the proposal does not make clear why a different legal basis is needed for the collection of biometric identifiers and for the processing thereof. It states that 'this proposal … deals with the collection of biometric data whereas the VIS proposal covers the transmission and exchange of data'. ([2]) However, from a data protection point of view, processing of personal data includes the collection thereof. Regulating operations in a chain of activities in different legal texts may be detrimental to the clarity of the regime. This is a problem for data subjects (to be affected by this proposal) as well as for democratic scrutiny of the system. It is indeed increasingly difficult to have the full picture in this area, where different pieces of legislation regulate what is basically the same data processing.

### 2.4. **Exemptions from fingerprinting**

This concern is very well illustrated by the question of the categories of persons exempted from the obligation to provide fingerprints, and especially in the case of young children.

The admissibility of the fingerprinting of young children should be discussed in the light of the purpose of the VIS itself. In other words, imposing the taking of biometric identifiers on some categories of persons or exempting them from this obligation, must be a proportionate measure in the framework of the visa policy and related objectives as stated in the VIS proposal. This proportionality should be assessed in a democratic procedure.

It should also be assessed in the light of the use to be made of these fingerprints, as described in the VIS proposal. Biometrics will be used for either verification or identification purposes: a biometric identifier could be judged technically suitable for the one and not for the other. The processing of fingerprints of children below the age of 14 is usually seen as reliable for verification only. This should influence the analysis of this proposal, but, again, the necessary elements are to be found in the VIS proposal (and are not yet decided upon).

In conclusion, the EDPS strongly advises that the exemptions to the taking of biometric identifiers in the VIS Regulation be strictly regulated, for reasons of clarity and consistency. The regulation of the collection of biometric identifiers and especially fingerprints in this case should be seen as ancillary to the main legal instrument and therefore addressed in the main document itself.

---

([1]) The fact that the legal basis is different — Article 62 (2) b) ii for the CCI, Article 66 for the VIS proposal — does not prevent the legislator from dealing with this matter in the same text.

([2]) Explanatory Memorandum, page 5

### 2.5. **Age of visa applicants**

The proposal states that only those children under the age of 6 will be exempted from the obligation to provide fingerprints. This raises many questions (regardless of whether this will be in the VIS or the CCI proposal).

First of all, the EDPS takes the view that a generalised fingerprinting of children cannot be seen as a mere technicality and should require a serious democratic debate in the appropriate institutions. Such a decision should not be based only on technical feasibility, but also, at least, on the benefit it would represent for the implementation of the VIS. However, with the exception of very few member States, there does not seem to be a public debate on this question presently, which is highly regrettable.

It must also be recalled that the VIS is established in principle with the objective of facilitating the visa procedures for bona fide travellers (the majority of travellers). Therefore, aspects of convenience and ergonomics should be taken into account ([1]). The use of biometric identifiers whether in the visa application procedure or at border controls should not make complying with visa procedures for children exceedingly difficult.

Finally, it should be recalled that all biometric identification systems have technical imperfections. The scientific literature does not present conclusive evidence that fingerprinting of children below the age of 14 can provide for reliable identification. The only experiences conducted so far on a large population are the Eurodac and US-Visit systems. Interestingly enough, both systems use fingerprints of children from the age of 14 upwards. Fingerprinting of children below that age should be supported by studies proving their accuracy and usefulness in the context of such a large scale database as VIS.

In any case, it would be advisable to use young children's fingerprints rather for one-to-one comparisons than for one-to-many comparisons. This should be regulated explicitly.

Finally, most of the remarks made here above do not concern only children, but also the elderly. The accuracy and usability of fingerprints decrease as people grow older ([2]) and aspects of convenience and ergonomics are also especially relevant.

### 2.6. **Photographs**

The same could be said about photographs, for which no age limit is foreseen either in this proposal or in the VIS proposal. However, it could be asked whether pictures of children taken before they have their adult features, are really useful whether for identification purposes, or even for verification purposes.

Facial recognition of children (whether automated in the future or 'human') based on reference pictures that are a few years old is likely to be problematic. Even if the technology of facial recognition makes significant progress, it is very unlikely that software will be able to compensate for the effect of growth on children's faces in the near future. Therefore, it should be clarified in the VIS Regulation that photographs can only be used as a supporting element for the verification or identification of individuals as long as the technology of facial recognition is not reliable enough, bearing in mind that this is likely to be the case for children in a more distant future.

Generally speaking, for both the biometric identifiers, the EDPS recommends giving serious consideration to the question whether the advantages (fighting illegal immigration and smuggling of children) outweigh the above mentioned drawbacks.

### 2.7. **Other exceptions**

The proposal states that applicants 'where fingerprinting is physically impossible' shall be exempt from the requirement to give fingerprints.

---

([1]) As underlined in a study commissioned by the Dutch government, in J.E. DEN HARTOGH et al., *How do you measure a child? A study into the use of biometrics in children*, 2005, TNO.

([2]) See e.g. A. HICKLIN and R. KHANNA, *The Role of Data Quality in Biometric Systems*, MTS, 9 February 2006.

The EDPS has already underlined in his opinion on the VIS proposal that this situation concerns a significant number of persons: up to 5 % of the population is said to be unable to enrol. On a database with 20 000 000 entries a year, it means that there could be up to 1 000 000 cases a year of difficulties in enrolling. This should certainly be borne in mind when analysing this proposal. Moreover, the EDPS insisted on the need for efficient fallback procedures:

*'Fallback procedures should be available to constitute essential safeguards for the introduction of biometrics as they are neither accessible to all nor completely accurate. Such procedures should be implemented and used in order to respect the dignity of persons who could not follow successfully the enrolment process and to avoid transferring onto them the burden of the system imperfections.'*

The proposed regulation provides for the introduction of the mention 'non applicable' in the VIS in these cases. This is certainly welcome. However, it could be feared that an inability to enrol could more easily lead to the refusal of the visa. If a very high percentage of inability to enrol leads to a denial of visa, it is not acceptable.

Therefore, a provision should be added to the VIS Regulation to the effect that an impossibility to enrol shall not automatically lead to a negative opinion on the issuance of the visa. Moreover, special care should be taken in the reporting foreseen in the VIS Regulation to address this issue: a high number of visa denials linked with physical impossibility to enrol should be monitored.

## 3. **OUTSOURCING OF VISA APPLICATIONS**

In order to ease the burden on each Member State (due inter alia to the cost of the purchase and maintenance of equipment), the proposal makes several cooperation mechanisms possible:

— co-location: staff from one or more Member States process the application (including biometric identifiers) addressed to them at the diplomatic post and consular mission of another Member State and share the equipment of that Member State;

— Common Application Centres: staff of diplomatic missions of one or more Member States are pooled in one building in order to receive the visa applications (including biometric identifiers) addressed to them;

— Finally, the proposal envisages that reception of the application form and taking of the biometric identifiers could be carried out by an external service provider (this option appears to be a last resort for Member States which cannot use one of the two other possibilities, although this is not entirely clear).

The proposal goes to great lengths to ensure that only reliable external service providers can be selected and that these providers must be able to take all necessary measures to protect data against 'accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (…)' (Article 1.B.2 of the proposal).

This provision is drafted with great care and attention for data protection, which the EDPS welcomes. However, having the processing of visa applications carried out by an external service provider in a third country has a number of consequences in terms of the protection of the (sometimes very sensitive) data collected for issuing visas.

The EDPS underlines especially the following:

— it may prove very difficult, perhaps even impossible to perform background checks on employees due to the third State legislation or practices;

— similarly, imposing sanctions on employees of an external provider for breach of privacy legislation will not necessarily be possible (even if contractual sanctions can be applied to the main contractor);

— the private company may be affected by political unrest or changes and not be in a position to fulfil its obligations in terms of security of the processing;

— effective oversight could be difficult to put in place although it would be even more necessary with external partners.

Therefore, any contract with external service providers should contain the necessary safeguards to ensure data protection compliance, including external audits, regular spot checks, reporting, mechanisms ensuring liability of the contractor in case of breach of privacy regulations, including the obligation to compensate individuals where they have suffered a damage deriving from an action of the service provider.

In addition to these concerns, may be even more importantly, one should be aware that Member States will not be able to guarantee the protection of the outsourced data processing (or of the data processing carried out in a Common Application Centre if this is done in a building outside diplomatic premises) against a possible intervention (e.g. search or seizure) by the applicant country's public authorities ([1]).

Indeed, external service providers will, despite all other contractual provisions, be subjected to national law of the third country where they are established. Recent events concerning access by authorities from a third State to financial data processed by an EU company show that the risk is far from theoretical. Moreover, this could involve a major risk for the individuals concerned in some third States who would be keen to know which of their citizens have applied for a visa (for political control on opponents and dissidents). Staff from a private company, in most cases probably local staff, would not be in a position to resist pressure from the government or law enforcement agencies of the applicant countries requesting data from them.

This is a major weakness of this system compared to the case where data are processed on the premises of a consular office or diplomatic post. In that case, data would be protected under the Vienna Convention of 18 April 1961 on Diplomatic Relations. Article 21 of this Convention stipulates that:

> *'The premises of the mission shall be inviolable. The agents of the receiving State may not enter them, except with the consent of the head of the mission. (…) The premises of the mission, their furnishings and other property thereon and the means of transport of the mission shall be immune from search, requisition, attachment or execution'.*

Moreover, according to Article 4.1.b of Directive 95/46/EC, national provisions implementing the Directive would also explicitly apply to this processing of personal data, reinforcing the protection.

It seems therefore evident that the only effective way to protect data concerning visa applicants and their (EU citizens or companies) sponsors is to grant them the protection ensured under the Vienna Convention. That means that data should be processed on the premises enjoying diplomatic protection. That would not prevent Member States from outsourcing the processing of visa applications, as long as the external contractor can carry out its activities on the diplomatic post's premises. This would also be true for Common Application Centres.

Therefore, the EDPS would strongly advise against the possibility to outsource the processing to external service providers as foreseen on page 15 of the proposal, new point 1.B.1.b). In this regard, acceptable options are:

— outsourcing the processing of visa application to a private company as long as it is located in a place protected under diplomatic status;

— outsourcing only the provision of information to a call centre as provided for in proposed point 1.B.1.a).

## 4. **CONCLUSION**

The EDPS welcomes the fact that this proposal to amend the Common Consular Instructions is to be adopted in co-decision, thereby enhancing the democratic scrutiny in an area where this is certainly much needed.

([1]) This problem exists already with the processing of applications by travel agencies; however, it is even more sensitive since biometric data are involved, and because the recourse to a travel agency is in principle not mandatory.

On the substance, the EDPS recommends the following:

— the exemptions of the obligation to provide fingerprints should be dealt with in the VIS Regulation rather than in the CCI, in order to ensure clarity and consistency of this regime;

— the age limits for fingerprinting and photographs should be given careful consideration, taking account of aspects of feasibility but also of considerations of ethics, convenience and accuracy;

— photographs should not be considered as a 'stand alone' identification method but only as a supporting element;

— outsourcing the processing of visa application to a private company should be admissible only if it involves a place under diplomatic protection, and is based on contractual clauses providing for effective oversight and liability of the contractor.

Done at Brussels, 27 October 2006

Peter HUSTINX

*European Data Protection Supervisor*