11224/04/EN
WP 96

Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)

Adopted on11 August 2004

Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS)

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:

INTRODUCTION

The Thessaloniki European Council of 19 and 20 June 2003 confirmed that "a coherent approach is needed in the EU on biometric identifiers or biometric data, which would result in harmonised solutions for documents for third country nationals, EU citizens' passports and information systems VIS and SIS II" and invited the Commission "to prepare the appropriate proposals, starting with visas".

At the end of September 2003, the European Commission submitted a 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 respectively. On 18 February 2004, it also submitted a draft Regulation on standards for security features and biometrics in EU citizens' passports.

The proposed amendment to the uniform formats for visas and residence permits essentially involves asking the Member States, on the one hand, to bring forward to 2005 the target date for the obligatory inclusion of a photograph in visa stickers and residence permits (originally scheduled for 2007 in the Regulations adopted in 2002) and, on the other, to include henceforth, as obligatory elements, two items of biometric data stored on a highly secure medium (contactless chip), i.e. a full-face digital photograph of the holder as the principal element for biometric identification together with two digital images of the holder's fingerprints taken with the fingers flat. According to the explanatory memorandum, the number of fingerprints could be increased on the basis of experience and the quality of the results obtained.

The biometric data incorporated into visas and residence permits should be made interoperable and entered into the European information system on visas (VIS). Similarly, the digital fingerprints of the persons referred to in the Schengen Convention would be entered into the Schengen information system (SIS II).

[1] Official Journal L 281, 23.11.1995, p. 31, available at: http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

Both SIS II and VIS are currently being set up[2]. The preparation of the European information system on visas (VIS) resulted in the adoption by the Council on 19 February 2004 of Conclusions providing general guidance that the Commission is invited to take into account when drawing up a proposal for the legal framework for the establishment and operation of this system. These Conclusions state that at a later stage, in coherence 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.

Shortly afterwards, in its Declaration on Combating Terrorism of 25 March 2004, the European Council provided for optimisation of information systems as part of the strengthening of the existing cooperation between Member States. In particular, the Declaration states that "the Commission and the Council are urged to take forward work on the Visa Information System (VIS) in line with the conclusions adopted in February 2004", thus stressing the need for swift action.

Answering this concern for speed, the Council recently adopted a decision establishing the Visa Information System (VIS) on 8 June 2004[3], thus providing the legal base necessary to permit the engagement of the corresponding financial means.

In addition, in the same Declaration of 25 March 2003, the European Council calls on 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.

All initiatives in this field are likely to have a major impact on the fundamental rights of the persons concerned (that is to say, every foreign national who applies for a visa – in other words, tens of millions of people). When future decisions are taken on setting up and implementing these new European information systems, due account must be taken of the principles of data protection enshrined in Article 8 of the European Charter of Fundamental Rights and referred to in Directive 95/46/EC and national legislation.

This document should, therefore, be understood merely as a preliminary opinion. It primarily concerns the proposals for regulations on uniform formats for visas and residence permits, for which the Working Party has been made formally responsible by the European Commission. The Working Party also comments on the points of principle raised by the Council's conclusions of 20 February 2004 on the establishment of an information system on visas (VIS), in the knowledge that the invitations to tender for this system are already under way. This global approach is in line with both the Commission's wishes and actual wording of Article 30 of Directive 95/46, which gives the Working Party general competence on proposed Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data.

The Working Party stresses, in this respect, that it needs to be consulted before any proposals are drawn up in this area, since only if there is genuine transparency in the

---

2 Cf. Commission Proposal of 11 December 2003 for a Council Regulation on standards for security features and biometrics in EU citizens' passports COM/2004/0116 final, which concerns the development of SIS II and synergies with the VIS information system.

3 Council decision of 8 June 2004 establishing the Visa Information System (VIS) (2004/512/EC)

processes under way will it be able to perform the functions assigned to it by the Directive.

Finally, the questions relating to the possible creation of a centralised database containing the biometric data collected from passport holders is outside the scope of the present document and will be dealt with separately. These questions will be examined by the Working Party in the near future.

1. GENERAL CONSIDERATIONS ON THE INCLUSION OF BIOMETRIC ELEMENTS IN RESIDENCE PERMITS AND VISAS AND THE SYSTEM OF INFORMATION ON VISAS (VIS)

The Working Party understands the concern about combating "visa shopping" and "identity theft", which have most unfortunate consequences for the victims.

However, in accordance with the points made in its working document on biometrics adopted on 1 August 2003[4], if biometric information were included in visas and residence permits and the corresponding personal data processed, a number of principles would have to be observed with a view to protecting the fundamental rights and freedoms of persons, particularly as regards their rights concerning processing of their personal data. Respect of these principles is particularly essential in connection with the processing of biometric data which, by their very nature, provide information on specific persons, especially as some can leave traces in people's everyday lives, without the people in question knowing that they can be collected (digital fingerprints are a notable example).

In accordance with Article 6 of Directive 95/46/EC, therefore, personal data must be collected only for specified, explicit and legitimate purposes and may not be further processed in a way that is incompatible with those purposes. Furthermore, the data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed (principle of purpose).

Respect of these principles first of all calls for a clear definition of the purpose for which the biometric data are collected and processed. The definition of this clear and explicit purpose would then make it possible to assess the legitimacy of including biometric data in visas and residence permits by permitting an assessment of the proportionality of collecting and processing these data in the light of this original purpose.

On this point, in application of the principle of purpose, the Working Party would point out that the growing interest in the application of biometric identification techniques calls for an extremely careful analysis of the legality of processing such data for identification purposes, since biometric data intrinsically involve genuine risks for the persons concerned if they are lost or used for purposes other than those for which they were intended. In particular, there is a not inconsiderable risk that an individual whose digital fingerprints have been collected does not otherwise communicate his or her real identity, particularly if the circumstances under which the fingerprints were collected do not guarantee perfect reliability; the hijacked identity would then be permanently associated with the digital fingerprints in question. Consequently, given these risks, an

[4] MARKT/10595/03/EN – WP 80

analysis of the possible faults in these systems as regards appropriate identification of persons is vital and should be conducted before processing of this kind is carried out (some of the proposals made in this field did not provide for this).

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.)

In this respect, the Working Party has great reservations, especially with regard to proportionality issues, about 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.

The Working Party also stresses the problems of reliability that could arise from the creation and interrogation of such a large database, and the potentially harmful consequences for the persons concerned[5].

The Working Party would also, therefore, like to know what studies of the scale and seriousness of these phenomena revealed compelling reasons of public safety or public order that would justify such an approach, and whether alternative approaches that did not involve such risks had been or could be studied.

In addition, all the appropriate guarantees have to be put in place to ensure that the data are not used in a manner that is incompatible with these purposes. As the Working Party pointed out in its previous working document, 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.

Finally, it should be borne in mind that, 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. The Working Party takes the view that these requirements may not be circumvented by the introduction of broad, multiple purposes. In other words, such purposes can be legitimate only if the principles mentioned above have been specifically applied to each of them.

---

[5] The possibility of finding the data relating to a specific person in a biometric database would decrease in proportion to the increase in the volume of data that the base contained, even though the search is made by automatic means. In this respect, it should be borne in mind that the number of visa applications that would be recorded in VIS on the basis of a five-year storage period would be around 100 million.

2. PROBLEMS CONCERNING THE IMPLEMENTATION OF EUROPEAN PROJECTS FOR INCLUDING BIOMETRIC ELEMENTS IN RESIDENCE PERMITS AND VISAS AND THE SYSTEM OF INFORMATION ON VISAS (VIS)

2.1 PROBLEMS CONCERNING DRAFT REGULATIONS ON UNIFORM FORMATS FOR VISAS AND RESIDENCE PERMITS

2.1.1 THE PURPOSE OF INCLUDING BIOMETRIC ELEMENTS IN RESIDENCE PERMITS AND VISAS

- The purpose of including these elements is initially "to establish a more reliable link between visas or residence permits and their holders"[6] by comparing, without recourse to a database, the data contained in the document and those of the person bearing it;
- in the longer term, when the infrastructure has been decided on and put in place, "to consult databases"[7].

The Working Party considers the first of these aims to be legitimate but thinks that it should be stated in the texts of the two Regulations, since it is on the basis of these aims that it will be possible to draw up a list of the persons authorised to access the stored data and the committee provided for in Article 6(2) of Regulation 1683/95 will be able to draw up the technical specifications for the incorporation of these data into the storage media and for access to the data.

However, given the lack of details on the precise scope of the second purpose, the Working Party thinks that this could give rise to major difficulties in connection with the principle of proportionality, which are related to those arising from the very establishment of the VIS (see below).

2.1.2 GENERAL CHARACTERISTICS OF THE BIOMETRIC TECHNIQUES USED IN THE UNIFORM FORMATS FOR VISAS AND RESIDENCE PERMITS AND THE CONSEQUENCES OF FALSE REJECTIONS

The Working Party stresses the need for a high level of reliability in the process of collecting and verifying the biometric data. Irrespective of how strictly the system has been tuned, the technologies applied should in any case lead to only a very low false-rejection rate, given the grave consequences for legitimate holders of documents.

The Working Party also thinks that there must be:

- measures enabling the persons concerned to have access to the data on the chip, if only to be able to check the contents particularly as regards their own biometric characteristics (Article 12 of Directive 95/46/EC);
- guarantees for persons 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);

---

6 Recital 2 and end of first paragraph of point 3 in the explanatory memorandum to the proposals for Council Regulations amending Regulations Nos 1683/95 and 1030/2002 laying down uniform formats for visas and residence permits respectively.

7 *Ibid.* end of sixth paragraph of point 3 in the explanatory memorandum.

- guarantees, particularly in the event of false rejections in border checks, that the persons in question will be informed of the reasons for the rejection and the means by which they may 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.

2.1.3 INTEROPERABILITY AND THE SECURITY OF THE DATA STORAGE MEDIUM FOR VISAS AND RESIDENCE PERMITS

The interoperability provided for in Article 4a of the proposals for Regulations would permit access to data stored on the chip in the form of images by an authority other than the one that entered the data. Given that the proposed medium is a contactless chip, the Working Party would like to receive, at an appropriate time before decisions are made to adopt the proposals, a document demonstrating that the specifications envisaged for the incorporation of data in chips and access to these data 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);

- the data cannot be accessed without the persons concerned being aware of it, by public bodies other than those legally authorised or by private entities; it would be appropriate to provide for encryption of the data in order to ensure confidentiality; access for reading the electronic elements could also be protected by an individual code known only to the holder;

- authorities with the right to access the data have access only to the information necessary for them to perform the tasks for which they are responsible.

2.1.4 PROVISIONS ON MACHINE-READABLE INFORMATION IN THE UNIFORM FORMATS FOR VISAS AND RESIDENCE PERMITS

The Working Party considers that the current wording of Article 4(2) of the proposal for amending the two Regulations, restricting the list of machine-readable information, is lacking in clarity:

> "No information in machine-readable form shall be included in the uniform format for visas, unless provided for in this Regulation or its Annex, or unless it is mentioned in the relevant travel document."

The Working Party would therefore like this provision:

- to list explicitly the personal data that could be presented in machine-readable form;
- to provide for informing the people concerned about the data that cannot be read directly in the document – in other words, the data stored on an electronic medium;
- to set out the measures to be taken so that people can check the information when the document is issued and subsequently, particularly by virtue of their access and correction rights.

2.2 PROBLEMS WITH THE VIS INFORMATION SYSTEM

The Working Party has already expressed in Point 1 reservations concerning the establishment of a central database containing biometric data on all non-nationals who apply for a visa or residence permit for the purpose of carrying out subsequent checks on illegal immigrants, if these data relate to traces that everyone leaves in their everyday life.

However, notwithstanding these reservations, and pending the work of the Commission and of the Committee set up by Article 5(1) of Council Regulation No 2424/2001 of 6 December 2001 on drawing up the rules governing the operation of the VIS, the Working Party would make the following observations regarding the principles underlying the conditions on which a database of this kind should operate.

2.2.1 THE GENERAL CHARACTERISTICS OF THE VIS INFORMATION SYSTEM

- **Purposes**

The purposes envisaged by the Council are very broad, as they cover not only preventing "visa shopping" and combating identity fraud through the exchange of information between Member States but also identifying persons without documents in irregular situations and contributing to internal security and the fight against terrorism. Some of these aims overlap with those of the Schengen II information system (SIS II), which is also being developed.

The Working Party therefore calls on the Commission to evaluate these purposes in the light of Point 1 of this opinion, particularly as regards the questions of the proportionality of the measures envisaged.

- **Centralised data and recipients**

So far, no list has been drawn up of the national authorities that will be able to access the data in the centralised database.
On this point, it is only when the purposes of the system are defined that it will be possible to determine the type of data the centralisation of which at the European level will be possible, as well as the list of the authorities having access to these data and the conditions of such access.

The Working Party would already draw attention to two types of data that should be examined particularly carefully as regards proportionality: the standardised reasons for rejection, a list of which has not yet been drawn up at European level, and information on persons sending invitations to or bearing the accommodation and subsistence costs of foreign nationals with a view to detecting clandestine immigration set-ups.

- **Access to data by non-member countries**

The Working Party gathers that certain Member States think that the authorities of non-member countries should be able to access information in the VIS database.

The Working Party considers that this would cause serious problems in connection with the rules laid down in Directive 95/46/EC, particularly as regards the principle of purpose and the requirements set out in Article 25 (1) on an adequate level of protection in the countries in which the recipients of these data are established.

- **The period for which data are kept in the VIS database**

In view of the principle of proportionality, the Working Party thinks that the period of five years for keeping data should be a maximum rather than a minimum.

The Working Party also suggests that more sophisticated retention criteria should be defined, taking into account the different situations which may occur in practice. 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. 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 in the different retention periods applied to the VIS.

Finally, the Working Party draws attention to the need, in application of the principle of purpose, to delete data on persons who have obtained the nationality of a Member State or a regular residence permit in a Member State[8].

- **Information for foreign nationals at the time of data collection**

The Working Party's mission is to contribute to the uniform application of Directive 95/46; it will make proposals, in the light of the characteristics to be covered by the VIS system and in application of the "fairness" criterion provided for in Articles 10 and 11 of Directive 95/46/EC, specifying the information to be supplied to the foreign nationals in question.

- **System security**

The Working Party would particularly stress the level of security that must be achieved in the process of developing the structure of the VIS. In accordance with Article 17 of Directive 95/46/EC, therefore, it must be stipulated that "appropriate technical and organizational measures" must be implemented "to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing".

It is vital that the level of security that must be achieved in the VIS be determined in the light of the risks that processing involves and the nature of the data to be protected. For example, it must be stipulated that data for transmission under the VIS system be encrypted so that they cannot be accessible to unauthorised third parties. There must also be access logs concerning in particular the processing of confidential and/or sensitive data, so that the authorities responsible can monitor the processing

[8] Cf. Article 25 of the Schengen Convention.

that takes place; these logs must be kept for an appropriate period before being deleted.

- **Interoperability of VIS and SIS II**

In its Declaration on Combating Terrorism of 25 March 2004, the European Council called on 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 Working Party would like to be able to comment in good time on the precise forms this interoperability will take, so that it can make an appropriate assessment of its implications for fundamental rights and freedoms where the processing of personal data is concerned. It therefore asks the Commission to inform it of its proposals so that it can analyse these aspects.

2.2.2 THE ROLE OF THE SUPERVISORY AUTHORITIES RESPONSIBLE FOR DATA PROTECTION

The European database VIS should be under the control of the European Data Protection Supervisor. The related national processing operations will be under the control of the national authorities.

When the cost of developing these systems at European and national level is evaluated, account must be taken of the new tasks of the supervisory authorities and the need to increase their resources so that their missions under the legislation may be effective.

Similarly, coordination and cooperation between these authorities will undoubtedly be necessary (in the event of complaints, for coordinated *in situ* checks etc.). This cooperation also presupposes adequate budgetary resources.

The Working Party invites the competent budgetary authorities to make commitments to increase the resources of the authorities responsible for data protection accordingly.

As the European Data Protection Supervisor should be declared competent for supervising the central part of the European information system on visas (VIS), it would be necessary to regulate in detail cooperation between this institution and the national supervisory authorities in order to guarantee the uniform application of the provisions on data protection.

The Working Party invites the Commission to examine this question and to inform it as soon as possible of its conclusions.

Under Article 46 of Regulation 45/2001, the European Data Protection Supervisor must cooperate with the national supervisory authorities referred to in Article 28 of Directive 95/46/EC and with the supervisory data protection bodies established under

Title VI of the Treaty on European Union ("third pillar"). He also participates in the work of the Working Party. [9]

2.3 CONCLUSIONS – THE ROLE OF THE ARTICLE 29 WORKING PARTY IN THE PROCESS OF DRAWING UP THE LEGAL FRAMEWORK FOR THE PROCESSING OF THE PERSONAL DATA IN QUESTION

The Working Party cannot overstress the importance that it attaches to being involved right from the preparatory stage in the drawing up of decisions on particularly difficult and sensitive matters, since if it is not informed of the proposed decisions or is informed too late, it will not be able to advise the Commission satisfactorily as provided for in Article 30 of Directive 95/46/EC, which is aimed at ensuring that, in the processing in question, a balance is maintained between the requirements of public security and the respect of the individual freedoms recognised by Community and national law.

The Working Party stresses that the balance to be struck between these two sets of requirements means that the fundamental principles of data protection must be respected, and in particular the principles of purpose and proportionality, as mentioned in Point 1 of this document.

The Working Party also notes that the various types of processing in connection with the various initiatives regarding international movements of persons[10], which are likely to involve interconnections, differ in terms of their purposes, nature and characteristics and therefore come under different fields of competency depending on whether they fall within the scope of the first or the third pillar.

This is why, at its meeting of 23-24 November 2003, the Working Party expressed the wish that a subgroup or task force be set up with the specific task of examining developments as a whole in the processing of personal data in this field.

In the absence of a clear indication as to whether the Commission would contribute to the organisation of this group, the representatives of the Article 29 Working Party, including the European Data Protection Supervisor, and the representatives of the supervisory authorities responsible for data protection in the third pillar have decided to set up this group on the occasion of the Spring Conference of European Data Protection Commissioners held in Rotterdam in April 2004.

The Group met for the first time in Brussels in June 2004 and will meet again regularly, with an aim to ensure that its members are informed fully and in good time on all the proposals and initiatives in question as they arise, so that they can examine them accordingly.

---

9 Art. 28 (6) of the Directive 95/46/EC does not mention the Supervisor but this is only due to the fact that at the time of the adoption of the Directive the institution of the Supervisor was not yet established.

10 For example, the proposal for amending the Regulations on uniform formats for visas and residence permits, the work under way on the VIS system and its alignment with the SIS II system, and the proposal for a Council Regulation (since adopted by the Commission on 18 February 2004) on security standards and biometric elements incorporated into the passports of the citizens of the European Union.

Therefore, the Working Party expresses the wish that, in particular, the Commission and the Council cooperate with this group to this end.

Done at Brussels, on11th August 2004

For the Working Party

The Chairman

Peter SCHAAR