

Opinion of the European Data Protection Supervisor on the draft Council Regulation (EC) laying down the form of the laissez-passer to be issued to members and servants of the institutions

(2006/C 313/13)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

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

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,

Having regard to the request for an opinion pursuant to Article 28(2) of Regulation (EC) No 45/2001 received from the Commission on 31 July 2006;

HAS ADOPTED THE FOLLOWING OPINION:

1. PRELIMINARY REMARKS

1. The Commission sent the European Data Protection Supervisor (EDPS) the draft Council Regulation laying down the form of the laissez-passer to be issued to members and staff of the institutions under cover of a letter dated 26 July 2006. The EDPS interprets this letter as a request for an opinion pursuant to Article 28(2) of Regulation (EC) No 45/2001.

2. The Protocol on Privileges and Immunities (PPI) of the European Communities, adopted on 8 April 1965 and annexed to the Treaty establishing a single Council and a single Commission of the European Communities, in particular Article 7 thereof, provides that the Council shall prescribe the form of Community laissez-passer (CLP), which shall be recognised as valid travel documents by the authorities of the Member States. This text constitutes the legal basis for the processing of the data (Article 5(a) of Regulation (EC) No 45/2001). The Council, which is the competent institution in this area, considers that the CLP no longer meets, at the present time, the security standards required for this type of document and that a complete overhaul is required in order to comply with the minimum standards of the ICAO (International Civil Aviation Organisation) and those required of the European passport (in particular biometrics), using new technologies to guarantee the greatest possible protection against falsification. For reasons of technical expertise, the Board of Heads of Administration has asked the Commission to study this question.

3. The EDPS considers it important to give an opinion on the proposal for a new CLP, since it envisages the inclusion, in a storage medium, of biometric data in interoperable and machine-readable formats. This opinion is the EDPS's opportunity to express his views on this issue, as he has already done previously in his opinions on the VIS ⁽¹⁾ and SIS II ⁽²⁾ programmes.

⁽¹⁾ 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 (COM(2004) 835 final), OJ C 181.

⁽²⁾ Opinion of 19 October 2005 on three proposals on the second generation Schengen Information System (SIS II) (COM(2005) 230 final, COM(2005) 236 final and COM(2005) 237 final), OJ C 91.

4. Biometric data are of a distinctive nature because they relate to a person's behavioural and physiological characteristics and can make it possible to identify that person with greater accuracy. In the EDPS's view, further processing falls within the scope of Article 27(1) of Regulation (EC) No 45/2001. Such processing must therefore be subject to prior checking by the EDPS, as it is likely to present risks to the rights and freedoms of data subjects by virtue of the nature of the data.

2. ANALYSIS OF THE PROPOSAL

2.1 General comments

5. The EDPS is being consulted on the basis of Article 28(2) of Regulation (EC) No 45/2001. However, as that provision is binding, this opinion should be mentioned in the preamble to the text.

6. The EDPS welcomes the fact that he is being consulted on the proposal for a new CLP, since the proposal forms one aspect of the policy for improving travel documents and enhancing their security with a view to making them more proof against falsification.

2.2 Biometric data

7. The proposal for a new CLP introduces the possibility of processing a new category of data which deserves special attention: biometric data. The EDPS recognises the importance of making the laissez-passer more secure in order to combat falsification and the fraudulent use of these documents. However, the introduction of biometrics and the corresponding processing of personal data must comply with a number of principles, the purpose of which is to protect the fundamental rights and freedoms of persons, in particular their rights with regard to the processing of their personal data. It is essential to comply with these principles in respect of the processing of biometric data which, by their very nature, give information on a specific person, especially as certain biometric data can leave traces in persons' daily lives and can therefore be collected without their knowledge (fingerprints, in particular).

8. Furthermore, there is a constantly increasing tendency to make use of biometric data in European Union information systems (VIS, SIS II, EURODAC, European passports, etc), without any concomitant close examination of the risks involved and the guarantees required. The Article 29 Working Party considered that data of this type [biometric] are of a special nature because they relate to a person's behavioural and physiological characteristics and can make it possible to identify him or her unambiguously ⁽¹⁾. The use of biometric data must therefore be accompanied by the adoption of additional guarantees and enhanced checking procedures.

9. The EDPS has already proposed, in an earlier opinion ⁽²⁾, that a list of common basic requirements should be drawn up, taking into account the fact that biometric data are sensitive by definition. It should be possible to apply the list to any system of any kind which uses biometrics.

10. In the same opinion, the EDPS stressed the importance of the enrolment phase for biometric systems. In the proposal as it stands, the origin of the biometric data and the manner in which they will be gathered are not described in detail. The enrolment phase is an essential step and it is not sufficient to define it by means of annexes; it directly affects the outcome of the procedure, i.e. the number of false rejections or false acceptances which might ensue.

11. For example, the EDPS recommends that easily accessible fallback procedures (of a technical nature and relating to the right of access) should be established and implemented during the enrolment phase, so that the dignity of persons unable to provide fingerprints acceptable to the system is respected.

⁽¹⁾ Working document on biometrics (MARKT/12168/02/FR — WP 80)

⁽²⁾ Opinion of 19 October 2005 on three proposals on the second generation Schengen Information System (SIS II) (COM (2005) 230 final, COM (2005) 236 final and COM (2005) 237 final), OJ C 91.

12. Article 2 of the proposal for a Regulation states that the storage medium shall contain *the personal data entered in the laissez-passer, a digitised facial image and fingerprints stored in interoperable formats*. Article 4 of the proposal states that the biometrics of the CLP shall be used only to *check the authenticity of the document and the identity of the holder* by means of comparable features directly available. In the light of these two articles, the EDPS wishes to make the following comments:

- On 28 February 2005, the European Commission adopted a 'Decision establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States'. On 28 June 2006 it also adopted a 'Decision establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States'; this Decision laid down additional technical specifications for the storage and protection of the fingerprints required. The EDPS recommends that these documents should be referred to in the Regulation as they concern the technical aspects of the biometric data, in particular the form of the fingerprints and the facial image.
- As the CLP are intended to be used in third countries, interoperability between the European systems and those of third countries must be guaranteed. The EDPS has already broached this issue in his opinion on the VIS system ⁽¹⁾. He would emphasise once again that the interoperability of systems must not breach the purpose limitation principle of the processing of data, and that any proposal in that area must be submitted to him.
- The proposal remains vague as to the possibility of storing fingerprints in an institutional database which thus becomes a register of the CLP issued. The Article 29 Working Party emphasises in its opinion 3/2005 ⁽²⁾ its opposition to the storage of biometric and other data of all the holders of a passport within the EU in a central database of European passports and travel documents. The EDPS feels that the same situation applies in the case of the CLP. The purpose of a CLP is to authenticate persons in third countries when they cross the border. Creating and setting up a central database containing personal data, in particular biometric data, of all persons authorised to receive a CLP is not justified, would violate the basic principle of proportionality, and should therefore be avoided. This issue should be distinguished from the processing of CLP application forms which are administered by the department responsible for issuing the CLP; we will return to this question later.

13. As regards the security of the CLP, the machine-readable data page is in conformity with ICAO document 9303 Part 1 (machine-readable passports), and its mode of issue is in accordance with the specifications applicable to machine-readable passports laid down there, and with the minimum security standards laid down in Regulation No 2252/2004.

2.3 Technical medium

14. Article 2(2) of the proposal for a Regulation lays down that the CLP *shall contain a storage medium [...]. The storage medium shall have sufficient capacity to guarantee the integrity, authenticity and confidentiality of the data*. This wording is in line with a Resolution of the European Parliament of 2 December 2004 ⁽³⁾ and this position is also supported by the Article 29 Working Party ⁽⁴⁾.

⁽¹⁾ See above page C 181/26.

⁽²⁾ Opinion 3/2005 on the implementation of Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

⁽³⁾ European Parliament legislative resolution on the proposal, submitted by the Commission, for a Council Regulation on standards for security features and biometrics in EU citizens' passports (COM(2004)0116 — C5-0101/2004 — 2004/0039(CNS)),
[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004AP0073\(01\):EN:HTML](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004AP0073(01):EN:HTML)

⁽⁴⁾ Letter of 18 August 2004 from the Chairman of the Article 29 Working Party to the President of the European Parliament, the Chairman of the LIBE Committee, the Secretary-General of the Council of the European Union, the President of the European Commission, the Director of DG Enterprise and the Director-General of DG Justice and Home Affairs (not published).

15. In order to comply with the decisions applicable to travel document security at European level, a basic access control is compulsory for all data stored in the chip, which means that all readers will also have to be equipped with a scanner which will deduce from the data entered in the passport the key required to open and read the chip. Furthermore, extended access control is compulsory for fingerprints. This system uses encryption which requires careful management of the access keys.

2.4 Purpose and proportionality

16. The introduction of biometric identifiers and the corresponding processing of personal data must comply with a number of principles aimed at protecting the fundamental rights and freedoms of persons, particularly their rights with regard to the processing of their personal data. It is essential to comply with these principles in respect of the processing of biometric data which, by their very nature, give information on a specific person, especially as certain biometric data can leave traces in persons' daily lives and can therefore be collected without their knowledge (fingerprints, in particular).

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

18. The principles of purpose (personal data should be collected and processed for specified and explicit purposes and their subsequent use may only be authorised in accordance with very strict conditions) and of proportionality (the processing of personal data is authorised only to the extent necessary and insofar as no other means involving a lesser breach of privacy is as effective) must be complied with when biometric data are processed. As already mentioned above, setting up a central database containing the personal data and, in particular, biometric data, of all persons authorised to receive a CLP would breach the principle of proportionality.

2.5 Information and access

19. The proposal for a Regulation contains a reference to the right to information (right of access, verification, rectification or deletion of data) of the persons to whom a laissez-passer is issued. However, the EDPS would like a reference to Article 33 of Regulation No 45/2001 on the right of Community staff to seek remedies to be added to recital 6 of the proposal.

20. The designation of the authorities and bodies authorised to consult the data present on the storage medium of the documents is governed by the relevant provisions of Community law, European Union law, or international agreements. The EDPS recommends that the authorities to whom this Regulation is addressed and the rights of access which are granted should be specified. It must also be guaranteed, in the interests of security of processing, that only the competent authorities may have access to the data stored on the chip.

21. There is no answer at present to other questions that arise where a CLP is checked in a third country: what data on the storage medium will third countries have access to? Furthermore, are protection measures taken to ensure that third countries do not retain the data which they have access to? At the very least, the questions concerning access to this information remain problematical.

3. OTHER COMMENTS

3.1 Issue of the CLP

22. The rules for issuing CLP, as laid down in Article 3 of the proposal, specify that CLP shall be issued by each institution, perhaps through a specialised body. However, one or more institutions may entrust to one of them the task of issuing their laissez-passer. It is also envisaged that the Commission should — following a call for tenders — designate a body to be responsible for printing blank CLP — and perhaps for personalising them by adding the personal data of the holder. Because of the special nature of the processing to be carried out and the necessary protection requirements associated with it, the rules governing the choice of the body responsible for processing will have to take special account of the principles laid down in Regulation No 45/2001 as regards the security and confidentiality of the data (Articles 21, 22 and 23 of the Regulation).

23. Without prejudice to the EDPS's opinion in the context of the prior checking procedure, which will follow notification ⁽¹⁾ by the data protection officer of the institution(s) responsible for the future processing of CLP, the EDPS wishes to set down, at this point, a number of general ideas as regards future processing.

3.2 The form

24. The documentation submitted for consultation does not contain any information about the form which persons interested in having a CLP (or authorised to have one) must fill in. However, in a case he dealt with previously, the EDPS reached the conclusion that the personal data processed when the old-style CLP are issued are not data relating to health, and that such data as might be linked to health (under the heading 'distinguishing marks') were not compulsory. Furthermore, the data subject's consent, defined in Article 2(h) of Regulation No 45/2001, applies. For this reason and so that he can form an exact picture of the procedure envisaged, the EDPS recommends that a copy of the CLP form should be attached to the dossier submitted for the procedure laid down in Article 27 of Regulation No 45/2001, and also any other document which facilitates the analysis of the case.

3.3 Data quality

25. Article 4(1)(c) of Regulation No 45/2001 lays down that the data must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. The data processed in the context of the procedure under consideration may be regarded as of significant magnitude (at least as regards the biometric data), which means that it is difficult to establish *a priori* and without knowledge of the specific case, whether they are 'adequate, relevant and not excessive'. It is therefore important that the persons who will process the data in the context of the various procedures are correctly informed of the obligation to comply with the principle laid down in Article 4(1)(c), and that they process the data in the light of that principle. In the context of the procedure laid down in Article 27 of Regulation No 45/2001, the EDPS will recommend drafting principles of conduct so that such persons are correctly informed of their obligations. He will also ask for specific training programmes to be set up on the issues associated with the processing of sensitive data.

26. In addition, the data must be accurate and, where necessary, kept up to date (Article 4(1)(d)). It is not possible, from the information submitted, to check whether the accuracy of the data will be guaranteed. Similarly, it is not possible at present to check that the procedure or the system will, in itself, fully guarantee the quality of the data. As stated in the preceding point, only an analysis under the Article 27 procedure will allow a check to be made that adequate protection measures have been put in place.

3.4 Data retention

27. The text states that the new laissez-passers would be valid for 5 years. However, it does not say how long the data relating to each application should be kept. Regulation No 45/2001 states that that data shall be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed' (Article 4(1)(e)). As stated above, the retention of biometric data in a database must be avoided. The EDPS therefore recommends separating the processing of the biometric data from the processing of the data provided on the CLP application forms. The latter may be kept as part of the normal procedure for processing CLP applications.

4. RECOMMENDATIONS

28. The EDPS welcomes the fact that he has been consulted on the Community laissez-passers. Nevertheless, the comments set out below should be taken into account:

— This opinion should be mentioned in the preamble to the Regulation, before the recitals ('Having regard to the opinion ...')

⁽¹⁾ On the basis of Article 27(3) of Regulation (EC) No 45/2001.

- Easily accessible fallback procedures must be implemented during the enrolment phase for the biometric data.
- The Commission Decisions of 28 February 2005 and 28 June 2006 'establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States' must be mentioned where they address the technical aspects of the CLP.
- The biometric data must not be stored in a central database.
- The content and format of the biometric data envisaged and the guarantees attached to the introduction of biometric data into the CLP must be described more precisely.
- Interoperability of the systems may not be introduced if it breaches the principle of limitation of the purposes of the processing of the data and any proposal in this area should be submitted to the EDPS.
- The principles of purpose and proportionality must be given particular attention in the processing of biometric data.
- In order to draw the attention of members and servants of the institutions to this issue, the reference to Article 33 of Regulation No 45/2001 on the right of Community staff to seek remedies should be added to recital 6 of the proposal.
- The EDPS wishes the proposal to specify that a limitative list be drawn up of the competent authorities that will have access to the data, also defining the rights of access they will be granted.
- The criteria for selecting the body referred to in Article 3 of the proposal must be carefully defined, in the light of the special nature of biometric data.
- The procedure for issuing the Community laissez-passer must be subject to prior checking by the European Data Protection Supervisor, pursuant to Article 27(1) of Regulation No 45/2001.
- The CLP application form should be provided so that data protection issues can be considered in the context of prior checking, and also any other document which facilitates the analysis of the case.
- The drawing up of principles of conduct should be recommended so that the persons responsible for processing the data are correctly informed of their obligations. Specific training programmes on issues relating to the processing of sensitive data should also be contemplated.
- It must be ensured that procedures are in place to guarantee data quality.

Done at Brussels, 13 October 2006.

Peter HUSTINX

European Data Protection Supervisor
