Visa Information System (VIS) and exchange of data between Member States on short-stay visas (VIS Regulation)

2004/0287(COD) - 23/03/2005 - Document attached to the procedure

OPINION OF THE EUROPEAN DATA PROTECTION SUPERVISOR

Given the sensitive nature of storing personal information on the Visa Information System, the European Data Protection Officer has been asked to give his opinion on the proposed legislative act. On balance, the EDPS approves of the VIS and recognises the need for creating a harmonised system of storing visa information, managed centrally by the EU. The report prepared by the EDPS states that, from a data protection point of view, the provisions have been drafted with due care and seem to be consistent and adequate as a whole. In spite of supporting the overall objective of the proposed legislative act, the EDPS has nevertheless identified a number of key concerns, regarding certain aspects of the proposed provisions, which are outlined below.

When examining the proposal, the EDPS took respect for an “individual’s private life” as the main point of reference for future discussions. Bearing this key principle in mind, the EDPS made the following observations:

- The VIS should be limited to the collection and exchange of data necessary for the development of a common visa policy. The information collected should be proportionate to this goal.

- The purpose of the VIS should be limited. This should be reflected in its content and who is authorised to use the system. Law enforcement agencies should not be given ‘routine’ access to the VIS given that it would not be in accordance with the stated purpose of the VIS (i.e. a common visa policy). The law enforcement authorities should be granted access on an *ad hoc* basis, under specific circumstances only and subject to the appropriate safeguards.

- The EDPS recognises the value and potential importance of using biometrics for storing information on an individual. Nevertheless, the Report highlights a number of fault lines associated with biometrics that indicate they can have far reaching consequences for individuals and society as a whole. Biometrics, for example, irrevocably alter the relationship between body and identity, in that they make the characteristics of the human body ‘machine-readable’ and subject to further use. Revocation of biometric data is almost impossible – a finger or face is difficult to change. Although this offers a number of possibilities for Member States’ authorities it also needs to be examined from the point of view of ‘identity theft’. The storage of fingerprints and photographs in a database linked to a stolen ID could lead to permanent problems for the real owner of his/her identity. Moreover, by its very nature, biometric data is not secret and can leave traces (fingerprints, DNA), which allows for the collection of this data – without the owner ever being made aware of this. For its part, the EDPS is concerned that the present proposal is being considered in the absence of a more widespread debate on biometrics. As a result one of the main recommendations of the EDPS is the introduction of more **stringent safeguards** for the use of biometric data in the proposed Regulation. These safeguards should be linked to the principle of limiting the information stored, restricting access to its content and boosting VIS security measures.

- The EDPS also makes some interesting comments regarding the technical imperfection of biometrics. Whilst it acknowledges that biometrics offers a number of advantages, some of the

advantages, such as data universality, permanence and usability, are never absolute. It is estimated that up to 5% of people would not be able to enrol on the system because they have no readable fingerprints – or no finger prints at all. The impact assessment report suggests that in 2007 there could be up to 20 million visa applicants. Were this to be the case, up to one million people will not be able to follow the normal enrolment process, with obvious consequences for visa applications and border checking. Further, given that biometrics can have an error rate of 0.5 to 1%, the EDPS points out that as a technology it can never offer an 'exact identification' of the data subject – as is suggested in the proposed Regulation. In light of this, the EDPS recommends that fallback procedures are developed and included in the proposal.

- On the matter of refusing a visa, the EDPS raises some concern over public health issues. The proposed provision, which would make public health a condition for entry, is considered by the EDPS as too vague.

- The EDPS calls for a precise and comprehensive definition of 'group members'.

- Regarding the matter of retaining data, the EDPS concludes that the provisions outlined in the proposed Regulation are reasonable. It must, however, be made explicit in the proposal that personal data must be entirely re-assessed for each new visa application.

- The EDPS points out that once the verification of identity has succeeded at border points, the Regulation does not make it clear for why further data is still needed.

- The EDPS calls for the creation of a complete list of user identities, which are to be kept permanently up-to-date by the Member States.

- Concerning the rights of the Data subject, the EDPS requests that data subjects should be informed about the retention period applying to their data.

- The EDPS requests an annual meeting with the national supervisory bodies of the VIS at least once a year; that technological implementation of data protection technologies should be done by way of a Regulation in accordance with the co-decision procedure and lastly, that the EDPS should be allowed to give advice on the Regulation's committee.

To conclude, the EDPS calls on all of the institutions involved in formulating the proposed Regulation to give due consideration to some of the issues it raises in this opinion, prior to its final adoption.