

Baroness Sarah LUDFORD
Membre du Parlement
Parlement européen
Bâtiment Altiero Spinelli
Rue Wiertz 60
B-1047 Bruxelles

Paris, 27 MAI 2008

N/Réf. : AT/YPA/SVT/SRE/EGE/ML/CS081042

Subject : Article 29 Working Party : outsourcing the collection of biometric data within the framework of visa applications

Dear Baroness,

I thank you for your letter of April 24, 2008 in which you have requested the views of the Article 29 Working Party on an informal document entitled "Options for the secure transfer of visa data between external service providers and local consulates of Schengen Member States" which has been prepared by the Commission services in order to address challenges of providing data security when the data is being handled outside the scope of diplomatic protection by the outsourced centres proposed in the proposal to amend Common Consular Instructions.

In its Opinion of 1 March 2007 on the initial proposal of the Commission (WP 134) the Article 29 Working Party (see also the EDPS opinion of 27 October 2006) has strongly advised against the possibility of outsourcing to external service providers and stated that this possibility should be considered as the option of last resort, depending on the organisation of diplomatic missions, but it is likely to present too many risks if it is not placed under the protection of diplomatic status and the full responsibility of the requesting Member State.

The Article 29 Working Party wishes to recall on a purely preliminary basis that it is not by principle opposed to the implementation of the externalisation of certain methods relating to the process of delivery of the visas. However, this outsourcing should in no case compromise the integrity of this process, and in particular its level of reliability and security as well as the guarantees surrounding the protection of personal data related to the applicants of visa.

Outsourcing activities shall comply with the principle of the security of the processing laid down in Article 17 of the Directive 95/46/EC. The purpose of this principle is to ensure that appropriate technical and organizational measures are implemented to protect personal data against accidental or unlawful loss, alteration disclosure or access, in particular where the processing involves the transmission of data over a network. These measures have to ensure an appropriate level of security as regards the risk represented by the processing and the nature of the data to be protected.

The Article 29 Working Party recommended that a strong and safe environment should be created for the reception of applications and the enrolment of biometric identifiers. Specific safeguards must be in place to ensure where enrolment functions are outsourced that liability remains with the competent visa authorities in the Member States and that processing is performed under strict supervision.

In the present case the operations will involve the processing of biometric data which in addition will be initially collected and processed by external service providers. Accordingly the technical measures to be implemented have to present the higher level required to ensure that the environment in which these processing operations complies offers the appropriate technical and organizational safeguards.

Collection of the biometric identifiers

Within this framework, the Article 29 Working Party estimates that the central point of this process relates to the collection of personal data. Indeed, to secure the transmission of personal, alphanumeric or biometric data is a minimal requirement for any processing of data, but does not constitute in itself a means of bringing the guarantees likely to avoid any risk of disclosure or diverted use of the data. The initial collection of the personal data must first of all be the subject of a high level of security and reliability.

The outsourcing of the collection of the data relating to the applicants of visa to external service providers can thus be considered only under conditions allowing the same level of security as the one which can be ensured in a consulate. The Article 29 Working Party estimates that it is only subject to this initial condition that the securisation of the data thus collected and transmitted between external service providers and the consular entities must be examined.

Moreover, in comparison with the purposes of the VIS defined in article 2 of its rules of procedures, the Article 29 Working Party considers that the obligations relating to security, the reliability and the relevance of the data has a particular importance. For all authorities recipients of the data processed within the framework of the VIS¹, the existence of a set of rules guaranteeing the transparency of the data processings implemented, the relevance and the reliability of information collected, is likely to reinforce the effectiveness of the device.

¹ These authorities are the competent authorities as regards visas; authorities in charge of controls at the points of passage at the external borders; authorities in charge of controlling the identity of the visa holder, the authenticity of the visa or the compliance with of the conditions of entry, stay or residence on the territory; competent authorities as regards asylum; authorities in charge of prevention, detection and investigation of the terrorist infringements and other serious penal infringements.

In the same way, the processing of biometric data relating to the applicants of visa imposes, considering the possible uses of these data and the serious risks of breach to privacy and the individual freedoms resulting from it, to give a particular importance to the implementation of guarantees of high security and confidentiality.

For all these reasons, the Article 29 Working Party estimates that the recourse to external service providers with regard to the collection of alphanumeric and biometric data of visa applicants, should be considered only as a last resort, in particular when the diplomatic and consular representations of the Member State concerned or other Member States, or of possible common centres of request, do not allow the implementation of the process of delivery of the visas under satisfactory conditions for the applicants.

Diplomatic protection

In any event, the enjoyment by the external service providers of the diplomatic protection defined by the Vienna Convention of April 18, 1961 on the diplomatic relations, is capable to guarantee the essential conditions of reliability and of data security, such as they are in particular specified in article 32 of the VIS rule of procedures.

This condition of diplomatic protection is necessary. According to the Article 29 Working Party, any provision of another nature without this diplomatic protection would not ensure a high level of security of the visa delivery process, as underlined in its opinion WP134 or by the European Data Protection Supervisor in its opinion of October 27, 2006.

Indeed, it would be very difficult to have a control on the employees of possible external service providers, because those which would be subjected to the constraints of the local law and that it would be thus always difficult to enforce potential sanctions, even if contractually envisaged. Moreover, the local private companies would always be subject to the political events of the country, and thus in position to satisfy their obligations. The effective monitoring by the authorities delivering authorization to external service providers would be also very difficult to set up locally.

The EDPS underlines rightfully that no contract, as binding as it can be, could sufficiently guarantee the protection of personal data by a satisfactory technical device, regular audits, mechanisms in the event of breach of contract, etc. Lastly, the Member States will not be able to really guarantee the outsourced processings against riots or local risings if these data processings are not hosted in diplomatic buildings, because the local companies would not have the means of resisting the pressures like a consulate or an embassy.

Ultimately, the Article 29 Working Party observes that the subcontracting of the collection of biometric data of visa applicants reveals a paradox: on the one hand one reinforces the level of reliability and security of the delivery of the visas by introducing biometrics but, on the other hand, the implementation of a device of collection which is not of the same level of security as the one which can be ensured in a consulate or a consular section of embassy, leads to weaken the reliability of the whole process.

Thus, the consequences resulting from this externalisation could be significant not only for the quality of the system of delivery and control of the visas, but also for visa applicants themselves if the conditions of confidentiality of their request and the data collected on this occasion, in particular biometric, were not sufficiently guaranteed.

On the technical options of data transmission

Under these conditions, the Article 29 Working Party estimates premature to approach the technical aspects of the transmission of the data, and in particular of the biometric data of visa applicants, between external service providers and Member States local consulates, since the question of the status conferred to these service providers is not the subject of a consensus.

The Article 29 Working Party reminds that in some Member States, the recourse to external service providers is not, for the time being, allowed (e.g. French system VISABIO).

Lastly, on the technical options suggested by the European Commission departments to secure the transmission of the data between external service providers and local consulates, the Article 29 Working Party estimates that, as the technical document underlines it, none of the solutions is completely satisfactory from a data confidentiality standpoint.

The first Option (*off-line solution*) appears in any event to offer a lower level of security concerning data transmission. The direct transfer and in real time on a USB key or a CD of the collected data, even strongly encrypted, and the sending of the support to the consulate for transfer of data in the data base, do not guarantee an impossibility of intercepting the data flows. The Joint Supervisory Authority of the Schengen system has underlined that such channel of communication presents too many risks and shall be forbidden.

Within the framework of options 2 (PKI solution) and 3 (secure web server solution), certain States or external service providers could also obtain access to encrypted data. Even by separating biometric flows from the other types of data, which is preferable in any case, these two options do not guarantee more impossibility of intercepting both flows and then re-correlate them. Although options 2 and/or 3 could be seen as offering a more secure environment in those cases where third country local legislation does not forbid (or requires) encryption of electronic communications and documents sent, by contrast none of these options will ensure the appropriate safeguards and guarantees to ensure the processing of these personal data against any alteration, access or loss of personal data either accidental or not. In other words, none of them would be likely to comply with the requirements set by the Article 17 of Directive 95/46/EC.

Therefore the Article 29 Working Party considers that unless these external providers are placed under "diplomatic protection" and their activity merely consists in collecting those personal data and transmitting them electronically to the consular office without storing any information or taking copy of it, none of the options suggested in the paper would allow to ensure on their own the necessary and required protection that the processing of these personal data required for the issuing of visas.

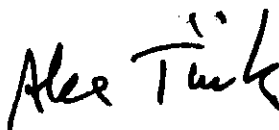
As mentioned above, no technical method of implementation of the collection and transmission of information by external service providers, does appear to provide the necessary guarantees as regards personal data, particularly biometric data.

Thus, a process of authorization of an intermediary, such as a travel agency or a company specialized in the collection of these data, to carry out the constitution of the files or the collection of biometric data, does not appear likely to guarantee the data security if the premises of the selected intermediary do not benefit from diplomatic protection. This observation remains valid even if the approval is limited in time and is granted on the basis of terms and conditions planning a certain number of controls, relating in particular to the information processing system. The same applies to the permanent presence of a consular agent in these buildings, in charge of supervising the work of the service provider.

Indeed, these methods do not allow the qualified public authorities to be really sure about the reliability of the collection, of the safeguarding of the confidentiality or the prevention of any diverted use of the data.

I thank you for the interest you have shown in the work of the Article 29 Working Party and I remain at your disposal to address any query you might consider to raise in order to ensure that this piece of legislation complies with Community data protection law.

Sincerely yours,

A handwritten signature in black ink that reads "Alex Türk". The signature is written in a cursive style with a horizontal line underneath it.

Alex TÜRK
Chairman of Article 29 Working Party