

Baroness Sarah Ludford, MEP
ASP 10G165
rue Wiertz
1047 Brussels

Carlos Coelho, MEP
ASP 08E146
rue Wiertz
1047 Brussels

By facsimile and email

Franco Frattini
Vice-President and European Commissioner for Justice and Home Affairs
European Commission
200 Rue de la Loi
Brussels

&

Minister Rui Pereira and Minister Alberto Costa
EU President in Office of Council of Ministers for Justice and Home Affairs
Council of the European Union
175 Rue de la Loi
Brussels

CC:

Jean-Marie Cavada, Chair of the LIBE committee
Peter Hustinx, European Data Protection Supervisor
Peter Schar, Chairman of the Art. 29 Working Party

Brussels, 22 November 2007

Dear Vice-President Frattini, dear President in Office of Council,

You will undoubtedly be aware of the massive data protection breach in the United Kingdom relating to the loss by a government department of two apparently unencrypted computer disks holding highly sensitive data of over 25 million UK citizens.

As rapporteurs on the Visa Information System (VIS) and the Schengen Information System II (SIS II) we were adamant in our call for effective data protection and data security provisions, excluding the copying or storage of sensitive data in mobile formats such as, for instance, diskettes or cd-roms.

In the negotiations of the SIS II, one of the major concerns of Parliament was exactly the problem of the so-called "technical copies" that lead to personal data stored off-line. The compromise with the Council was that all routine technical copies which lead to data stored off-line would have to be phased out, and that only in exceptional cases could a copy be made off-line if several rigorous criteria were met and they were destroyed after 48 hours. Similar considerations were made in the VIS, where Member States are excluded from keeping national copies of the VIS data and where a number of safeguards as regards data security have been put in place.

However, the need for effective and enforceable data protection mechanisms remains a major preoccupation and a top priority for Parliament. The extent of the challenges which evoke our concern can be illustrated by the fact that in the current discussions on the draft Common Consular Instructions/biometrics collection measure, Parliament has been provided with a document from the Commission in which offline copies on disc are still presented as a possible means of transfer of visa data, and that in a context in which encryption may be challenged by the host country.

The data protection challenges presented by the large scale biometrics data bases, such as VIS, SIS II and Eurodac, is compounded by giving law enforcement access to these data-bases.

Therefore, in view of the massive data protection and data security breach that the UK event has highlighted, we would ask you to draw the appropriate lessons in relation to current and future legislation, practice and monitoring of EU databases. It would we feel be appropriate for the Commission to draw up a green paper on the risks that exist and the safeguards needed to keep data safe, with of course the full participation of the Article 29 working party and the European Data Protection Supervisor, as a basis for a full and open discussion with the European and national parliaments, Member States and civil society.

We look forward to what we hope will be your positive response.

Yours sincerely,

Baroness Sarah Ludford, MEP

Rapporteur on VIS and CCI

Carlos Coelho, MEP

Rapporteur on SIS II