



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 5 February 2002

5969/02

LIMITE

**SIS 7
COMIX 79**

NOTE

from : Presidency
to : Working Party on SIS (EU/Iceland and Norway Mixed Committee)

No. prev.doc. 5968/02 SIS 6 COMIX 77
12156/01 JAI 99
14790/01 SIS 107 COMIX 767
14094/01 SIS 100 COMIX 742
6164/5/01 REV 5 SIS 11 COMIX 114

Subject: Requirements for SIS related to the Action Plan against Terrorism

In its conclusions of the meeting of 20 September 2001 concerning the measures to combat terrorism, the JHA Council agreed to examine whether to extend in the context of counter terrorism SIS access to other public services (conclusion 13), emphasised the important role of the Security and Intelligence Services in the fight against terrorism (conclusion 14) and invited those States participating in the SIS to provide more systematic input into the system of alerts under Articles 95, 96 and 99 of the Schengen Convention (conclusion 27).

Therefore, the following requirements have been listed in this document so that they can be discussed separately, with a view to reaching an agreement as soon as possible and implementing them quickly.

Simplifying procedures for introducing Article 99 alerts

In order to promote a better use of alerts pursuant to Article 99 of the Schengen Convention, as requested by the Council on 20 September 2001, it seems useful and justified to replace the procedures laid down in the Schengen *acquis* (Article 99 of the Convention and the SIRENE Manual) for introducing Article 99 alerts by a system simplifying the consultation mechanism.

As it seems useful to maintain the obligation for States to consult each other before introducing an alert pursuant to Article 99 and especially Article 99(3), there would be no need to amend the provisions of the Schengen Convention, but only to review the procedures set out in the SIRENE Manual.

This requirement would thus be taken care of in the legislative act modifying the SIRENE Manual.

Access to the SIS for security and intelligence services

The Council has also invited MS to exchange information on the practical measures adopted at national level to combat terrorism. They highlight controls at airports, cross-border controls, controls on express roads and controls at the external borders of the EU. In addition Council instructed the Working Party on Terrorism to draw up an inventory of such measures, in collaboration with Europol and to work out “alert and intervention” plans to deal with transfrontier terrorist acts.

Within several MS security or intelligence services have a statutory or defined responsibility to combat terrorism and several share this responsibility with police services. The role of the “authorities responsible for State security” is already recognised within the Schengen Convention with Article 99(3) providing for alerts issued on their behalf. In their report to Coreper (14193/01 SIS 101 COMIX 745) the Belgian Presidency highlighted the importance of defining “those authorities responsible for State Security”.

In the absence of such a definition it is the intention of these proposals to apply to those Security and Intelligence Services with internal security responsibilities allied to Justice or Home Affairs / Interior Ministries as opposed to military or other intelligence services with external responsibilities.

If an agreement in principle is reached on allowing these authorities access to SIS, the legislative act concerned will have to determine in detail:

- which services are covered: those Security and Intelligence Services with internal security responsibilities allied to Justice or Home Affairs / Interior Ministries;
- to what categories of data they can have access: all SIS data, including the restricted terrorist database (cf. infra);
- what purpose they can use the data for: information purposes with a view to national and international coordination of counter-terrorism and
- what data protection guarantees have to be provided: capacity of personnel, ...

Restricted access terrorist database

As for the proposal of giving access to the SIS to Security and Intelligence Services, the proposal of the creation of restricted access terrorist database has to be seen in the context of the overall strategy being developed post 11th September 2001 which calls for strengthening co-operation between police services and intelligence services and maximising the potential of existing instruments. The SIS is recognised as an efficient and robust means of quickly and securely communicating information [to the operational level] and it is therefore well suited to carry sensitive information. Every member State has specialist units/departments within the police service tasked with combating terrorism. It is intended that officers attached to such units should have access to an additional source of information in respect of terrorist suspects, without this being circulated widely to all law enforcement officers.

If an agreement in principle is reached on creating this restricted database, the legislative act concerned will have to determine in detail:

- what kind of information can be included in this restricted database: information in respect of terrorist suspects, ...;
- under which conditions this information can be introduced: legal basis for an alert, authority responsible for the alert, duration of the alert, ...;
- for what purpose this information can be used
- which authorities can introduce and/or access the data: specialist units/departments within the police service tasked with combating terrorism, Security and Intelligence services;
- and what other data protection guarantees need to be provided.