COUNCIL OF THE EUROPEAN UNION

Brussels, 25 March 2011

8118/11

Interinstitutional File: 2011/0023 (COD)

LIMITE

GENVAL 28
AVIATION 66
DATAPROTECT 18
CODEC 484

TRANSLATION PROVIDED BY THE GERMAN DELEGATION

NOTE

from:	German delegation
to:	Working Party on General Matters, including Evaluations (GENVAL)
No. Cion prop.:	6007/11 GENVAL 5 AVIATION 15 DATAPROTECT 6 CODEC 278 + ADD 1 + ADD 2
Subject:	Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime - German position

Germany would like to thank the Commission for its efforts in preparing the dossier to which Germany attaches great significance in terms of both policy and fundamental rights. In particular, Germany notes that the present draft addresses several key concerns which Germany expressed regarding the Commission's 2007 proposal for a Framework Decision:

- restricting its scope to international flights – **Article 1 no. 1 of the draft**,
- establishing a decentralized structure of central offices – **Article 2 no. 1 of the draft**,
- further reducing retention periods, in particular the period for storing full PNR data – **Article 9 no. 1 of the draft**,
- clearly specifying the different possibilities to process data – **Article 4 of the draft**.

However, Germany notes that more actual information should be provided to allow for a reliable assessment of the project, in particular its necessity. In this context, it would be advisable to examine existing possibilities for later access to PNR stored by air carriers. Moreover, we should check the information provided in the **explanatory memorandum** because some of it is apparently incorrect.

Nevertheless, Germany expressly welcomes the fact that the Commission has considered the comments of the European agency for fundamental rights on the proposal for a Council Framework Decision on the use of Passenger Name Records for law enforcement purposes.
Germany recognizes that the present proposal includes major improvements as regards the protection of fundamental rights (e.g. reduced retention period of five years, instead of ten, and retention and analysis of anonymized data).

Germany would like to provide meaningful input to the consultations on the proposal. To achieve a high level of protection of fundamental rights, the following requirements must be fulfilled:

- Reducing and specifying the **record**;

  Expressly and strictly limiting the air carriers' transfer obligations to data which they store in their own interest: The provision of **Article 6 no. 1, first sentence,** could be misunderstood because it implies that air carriers automatically store the data specified in the Directive. Clarification should be provided in Article 2(c).

- **Limiting the list of offences** to those offences for which it seems useful and appropriate to use PNR data given their severity and type.

- PNR data should be used for **real-time analysis** only if it is ensured that the **full (i.e. not anonymized)** PNR data are used exclusively for these purposes and only for the duration of the real-time analysis;

- **Non-anonymized data** must not be retained longer or for other purposes (no retention of full PNR data for 30 days);

- PNR data should be used "**pro-actively**" only if they are anonymized;
- PNR data should be used for the **purposes of threat prevention and law enforcement** with the **shortest possible** retention period, which must be significantly shorter than five years;
- We should add a provision stipulating that PNR data may be used as **evidence in criminal proceedings** only after prior consent of the country where the data were collected (guaranteeing legal assistance);
- We should store **only records of persons** who **raised suspicion** during the real-time analysis;
- Data should be stored only **anonymized**, and restoring full PNR data should require an independent prior examination by an entity which is not accountable to the head of the central office;
- **Strict requirements for using** PNR data **reactively:**
    - Full PNR data should be used for **law enforcement** only if the **individual offence is truly serious**;
    - Full PNR data should be used for **threat prevention** only if certain facts provide reasonable grounds to assume that there is a **specific imminent threat to the life, limb, or liberty of a person, to the existence or security of a Member State or to the prevention of a general threat**;
- Persons concerned should be **notified after their PNR data have been used reactively**, unless there are compelling reasons to the contrary or the notification would demand an unreasonable effort.

In addition to the concerns regarding fundamental rights, the proposal provokes some critical remarks and questions which will be presented during the discussions on the wording announced by the Presidency. One question will be why the criteria for real-time analysis (see Art. 4(3) of the proposal) are not defined more precisely. The current proposal creates great legal uncertainty for the parties concerned, which is even aggravated by the fact that the different Member States apply different criteria. This raises the question of how effective the system is given the different criteria in the Member States.

Germany's answers to the Presidency's questions:

1. The Presidency invites Member States to discuss whether they agree with the option of the Commission proposal for a decentralised system or whether, notwithstanding the arguments marshalled by the Commission, they would be in favour of a centralised system.

Germany shares the Commission's view that a decentralized system should be favoured over a centralized system. Germany agrees that a central European agency would need direct access to numerous national police and law enforcement databases, e.g. for the real-time analysis, which would be extremely problematic. However, for Germany the most compelling argument against a centralized system is that a central sovereign agency would have to be created which, depending on the scope, would have almost full access to important personal data of all European citizens travelling by plane, at least on international flights. In terms of privacy law, concentrating personal data in one agency would increase the system's potential for errors and misuse and is therefore rejected. In addition, Germany will insist on an independent entity which will have to decide on the transfer of records in the specified cases or the restoration of detailed data, for example. Supervisory bodies can be more effectively included in the existing judicial and administrative structures of the Member States; as national bodies (authorities or courts), they have profound knowledge of the respective national law.

2. The Presidency invites Member States to discuss the UK proposal and other possible alternatives for extending the scope of the PNR Directive in order to include the collection of PNR data from intra-EU flights.

Germany would like to point out that intra-EU flights have already been excluded in the previous drafts (2007 draft of a Proposal for a Framework Decision and its revisions). Including such flights would, in Germany's view, raise serious issues regarding free movement.

There is no reason why the Directive's scope should be extended in line with the UK proposal or the Presidency's alternative proposal.

Given the high security standards in Europe, it is not clear how analysing PNR data for the protection of specific flights against terrorist attacks could increase security.
But the most essential aspect is that including intra-EU flights would seriously restrict the citizens' freedom of movement and, given the higher proportion of travelling within the EU, create a level of surveillance which would no longer comply with fundamental rights. The options model proposed by the UK raises in particular the question of how to justify the partial restriction of the freedom of movement within the EU.
Moreover, the benefit of control systems such as PNR analyses strongly depends on alternatives for offenders. However, there are many alternative travel routes within the EU which are not subject to surveillance.

After an initial assessment we reached the conclusion that the UK proposal could not be implemented also for legal reasons: For example, to transfer data from Germany to the UK, German law requires sector-specific data protection. UK legislation cannot replace the necessary national legal basis. Germany is opposed to the idea of introducing a "preventive obligation" to create such a legal basis in case other Member States insist on the transfer of PNR also for intra-EU flights so that further bilateral agreements would have to be concluded.

Finally, extending the scope to include intra-EU flights could not be addressed separately; it would significantly affect almost all other provisions of the draft Directive, including the question of whether a dedicated Directive would have to be adopted for intra-EU flights. Therefore, further discussions do not seem useful at this point. Germany urgently suggests that discussions on the present Commission proposal be given priority. We may discuss the issue of intra-EU flights at the appropriate time in line with Article 17(a).

3. The Presidency invites Member States to discuss whether:

- *the proposed split between two retention periods with reduced access possibilities during the second period is acceptable*
- *the proposed retention periods are acceptable*

Germany is opposed to retaining full PNR data for 30 days and notes that a period of 24 hours is sufficient for real-time analyses of API data. There seems to be no reason why full PNR data should be stored after the real-time analysis. Full data are not necessary for the pro-active use, and for the reactive use they may be restored if the pertinent requirements are fulfilled. This would apply also for the exchange with other Member States. An exchange of the full PNR data does not seem necessary unless needed to respond to a specific and current threat pursuant to the Directive or to prosecute a specific offence. The retention period for anonymized data should be as short as possible. So far, no convincing arguments have been advanced as to why anonymized data should be stored for five years, which in our view is clearly too long