COUNCIL OF THE EUROPEAN UNION

Brussels, 2 May 2011

9502/11

Interinstitutional File: 2011/0023 (COD)

LIMITE

GENVAL 47
AVIATION 113
DATAPROTECT 38
CODEC 705

PROPOSAL

from:	Presidency
to:	Working Party on General Matters, including Evaluations
No. prev.doc.:	8458/11 GENVAL 33 AVIATION 78 DATAPROTECT 26 CODEC 545
on:	Proposal for a Directive of the Council and the European Parliament on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime - Discussion paper on data protection issues

1. On 3 February 2011, the Commission presented a 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. A first reading of the entire text of the Directive (except the Preamble) took place at the GENVAL meetings on 8 and 28 March 2011.

2. At the Council meeting on 11 April 2011, a discussion was held on whether intra-EU flights should be included in the scope of the draft Directive. Further to that discussion, the Presidency intends to continue preparatory work on the draft PNR Directive at expert level on the basis that the Directive should allow individual Member States the option to mandate the collection of PNR data with regard to targeted intra-EU flights and that the collection and processing of such data should be subject to the legal regime created by the PNR Directive. The possibility of inserting a review clause will also have to be studied[1]. The new draft prepared by the Presidency therefore includes an article (1a) on the inclusion of intra-EU flights[2].

3. As the Presidency and several delegations indicated during (the preparation of) the Council discussion of 11 April 2011, data protection is an issue in its own right regardless of any extension of the scope of the PNR Directive, which would take place on the understanding that the issue of data protection would need to be addressed. Following the Council meeting on 11 April 2011, the Council Legal Service produced an opinion on data protection questions related to the draft Directive[3].

4. The Presidency is fully aware of the fact that data protection will be at the heart of future discussions on this proposal, both within the Council and with the Parliament. A number of pivotal data protection questions, such as the need to demonstrate the necessity and proportionality of the PNR tool and the period during which data can be stored, are moreover relevant to other files as well, not only for political reasons, but also in view of possible litigation before the Court or national constitutional courts. At the same time, it needs to be kept in mind that the collection and processing of PNR data serves certain law enforcement purposes (set out in Article 4(2)) and therefore care needs to be taken that any data protection arrangements for the collection and processing of PNR data do not defeat the very law enforcement purposes they are supposed to serve.

---

1 9103/11 GENVAL 43 AVIATION 100 DATAPROTECT 34 CODEC 648.
2 8458/11 GENVAL 33 AVIATION 78 DATAPROTECT 26 CODEC 545.
3 8850/11 JUR 163 GENVAL 38 AVIATION 92 DATAPROTECT 30 CODEC 618.

5. The Presidency would therefore wish to focus the data protection debate on the following questions:

Need for PNR data

6. The usefulness and indeed the need for PNR data for law enforcement (including counter-terrorism) authorities has been thoroughly investigated in the context of the thematic work carried out with regard to the draft PNR Framework Decision during the French Presidency. Already in the first half of 2008, the Australian, Canadian and US authorities had given detailed presentations setting out, inter alia, the usefulness and need for PNR data. During the French Presidency of the Council (second half of 2008), the Multidisciplinary group on organised crime questioned in details various Member States services responsible for security. The operational services of the PNR databases already in place in the United Kingdom were heard, as were those of the French customs authorities, the Danish national police and the Danish intelligence services and the Belgian criminal police, which use PNR data in the context of pro-active activities within the domestic legal framework. All authorities testified that PNR data is a key means of combating numerous forms of serious crime, particularly those susceptible to detection when borders are crossed (activities linked to terrorism, trafficking in drugs, in endangered species and all types of illicit product, counterfeiting, trafficking in human beings, false passports, etc.). Numerous real-life examples were provided. Statistics adapted to the "PNR usefulness" question are not always available. However, the French customs authorities formally stated that each year between 60 % and 80 % of narcotic seizures at the international airports of Paris (roughly two tonnes annually) are directly attributable to the availability of PNR data[4].

7. Both from a political and from a data protection point of view, it is difficult to argue why the European Union would not equip itself with a PNR system whereas it allows third countries to use PNR data of EU citizens for certain CT and law enforcement purposes.

---

4 15319/1/08 REV 1 CRIMORG 184AVIATION 255 DATAPROTECT 86.

Range of data to be collected v proportionality

8. It is a basic principle that only those data that are needed for law enforcement purposes need to be collected. For certain types of data collected by private companies (PNR data being only one example) for purely commercial purposes which may be potentially interesting and in some cases indispensable for law enforcement purposes, the problem is that often it will not be known beforehand which data need are needed. At the same time, these private companies store such data only for a limited period of time. The main challenge is therefore to find a means by which the relevant data will still be available to law enforcement authorities when they need them after some time. In this context, at least the following elements are relevant: who stores the data, which data are collected and stored and for how long. There are obviously also other important data protection elements such as the need to have a robust data security system in place.

9. The proposal for a PNR Directive seeks to meet that challenge by obliging Member States to retain those data for a certain period of time in a database, held at the PIU. One could also envisage another solution, i.e. where the Directive would oblige air carriers to store the data for a certain period (a model followed by the 2006 Data Retention Directive), possibly combined with transmission of those data to the relevant Passenger Information Unit (PIU) for a short period (e.g. 24 hours as for API data) in order to allow the PIUs to carry out an assessment of passengers prior to their scheduled arrival (cf. Article 4(2) (a) and (b)).There appear, however, to be important drawbacks to such a model. Whilst it ensures that the government collects (per request to the air carriers) and stores only those data that it needs for the prevention, investigation and prosecution of offences (cf. Article 4(2) (c)), it would completely deprive the Member States of the possibility of creating new risk criteria (cf. Article 4(2) (d)). Moreover, it would be significantly more costly for the air carriers as they would have to bear the costs of storing the data.

10. It may be more realistic to build in the necessary data protection limitations by other means, namely a restriction of the data that are collected and stored and of the retention period.

11. Regarding data collection, following the Council discussion on 11 April 2011 Member States may be given the possibility of collecting and processing PNR data on *targeted* intra-EU flights. For international flights, the Commission proposal provides that, after a transitional period (Article 16), PNR data on *all* flights must be collected. At least from a data protection point of view, this distinction seems difficult to justify. If one accepts that for intra-EU flights, Member States are allowed to collect data only on targeted flights, i.e. flights for which there is a particular law enforcement risk, it seems disproportionate to collect PNR data on all international flights.

    The Presidency therefore invites delegations to consider whether the collection of PNR data on international flights could be limited to targeted flights. Delegations may also wish to reflect on whether (and how), from a data protection point of view, the possibility to target flights should be circumscribed in the draft Directive.

Retention period

12. Regarding data retention, discussions in the GENVAL Working Party so far have shown a divergence of opinions between Member States on what is the appropriate period for retaining data. It is likely that an even greater divergence of opinion exists within the European Parliament. Obviously data protection concerns plead in favour of a retention period which is as short as possible, whereas from an operational point of view the longer the data are available to law enforcement authorities, the better. It is difficult to say where the right balance can be struck, but it appears that PNR data can only significantly help to achieve the purposes referred to in Article 4(2)(c) and (d) if the relevant data are stored for long enough. This seems to be at least a number of years. The Commission proposed that the retention period be split up in two sub-periods (30 days + five years), with reduced access possibilities during the second sub-period.

    The Presidency invites delegations to reflect on whether (and how) reduced access possibilities offer substantial (or only presentational) data protection advantages. In this context, the technical question of how one can ensure that as much personal data are "masked out" and how one can/should restrict access by individuals to PNR data also merits further reflection.

Purpose limitation

13. Another important data protection limitation is the purpose for which PNR data can be used. The draft PNR Directive limits these purposes in two ways: by describing the functional activities for which the data can be used (Article 4(2)) and by describing the categories of offences the government seeks to prevent, investigate or prosecute through those activities: terrorist offences and serious crime. Regarding these offences, the Commission has sought to limit the scope of the concept of serious crime in two ways. Firstly by allowing Member States to exclude minor offences from the list of offences of Article 2(2) of the EAW Framework Decision. Secondly, by limiting the possibility of using PNR data for screening passengers against pre-set risk criteria or for developing such criteria for *transnational* serious crime. During the discussions in the GENVAL Working Party the latter distinction was criticised by several delegations.

The Presidency invites delegations to reflect on how the operational needs for the use of PNR data can be reconciled with the data protection requirement to limit the offences against which PNR data can be used. Delegations are also invited to consider whether such limitations can be left to the national law of Member States or should be fully circumscribed in the draft Directive.

Link with API (and other available) data

14. In the context of the thematic work carried out with regard to the draft PNR Framework Decision during the French Presidency, it was clearly demonstrated that PNR data offer supplementary information to that already available. In this regard the following was stated:

> "Because of the special nature of PNR data (all information about a travel reservation) and the possibility of access to it well before the flight lands, such data is complementary to other existing control or investigation tools, not superfluous to them. Its use gives access to specific information about offenders' behaviour, such as the itineraries for and frequency of their journeys, the circumstances in which their plane tickets are bought (travel agency, means of payment, credit card details, group purchases, etc.) and other matters connected

with the trip (hotel reservation, car hire etc). It makes it possible to detect offences because of suspicious behaviour, to find those suspected of crimes, to reveal links between a person and a known criminal, or links between a person and a particular criminal case. The establishment of a PNR database offers both opportunities to analyse behavioural tendencies in criminal circles, on which basis the criminal risk on particular flights can be assessed, and opportunities to provide information for investigations by intelligence services, customs, police and the criminal justice system. It allows the proactive use of the information contained in it, with the aim of preventing crime and detecting crimes which have been committed or are being planned; also, thanks to the later use of data which has been stored, it may help to clear up unsolved crimes"[5].

15. During the work on the draft PNR Framework Decision, the operational importance of combining the use of PNR data with API data was also highlighted on several occasions. From a data protection point of view, the availability of API data to law enforcement authorities, but also other data such as those contained in the SIS or VIS, makes it necessary to demonstrate the operational need for the additional availability of PNR data. Such operational need may be easier to argue in the case of a targeted collection of PNR data than in the case of collection of PNR data on (all) flights, but there may be other ways of limiting the use of PNR data for pre-arrival screening.

The Presidency therefore invites delegations to reflect on whether the use of API data should be mentioned in this Directive and whether the use of PNR data for comparing against relevant databases (Article 4(2)(b)) needs to be limited in the draft Directive.

---

[5] 15319/1/08 REV 1 CRIMORG 184AVIATION 255 DATAPROTECT 86.