Translation of covering letter

Dated: 5 April 2011

From: Ms Barbara Prammer, President of the Austrian National Council (Nationalrat)

To: President Barroso

Annexes

Ref: 13026.0036/11-L1.3/2011

Dear Mr Barroso,

At a meeting on April 2011, the Nationalrat Standing Subcommittee of the Main Committee on EU Affairs adopted the attached **Communication under Article 23f(4) of the Federal Constitution (B-VG)** during consultation on

COM(2011) 32 final -

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
(45269/EU XXIV.GP)

COMMUNICATION

of the Nationalrat Standing Subcommittee of the Main Committee on EU Affairs of 5 April 2011

under Article 23f(4) of the Federal Constitution (B-VG)

COM(2011) 32 final -

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
(45269/EU XXIV.GP)

"Maintaining public security is fundamentally the task of the Member States. No-one would dispute that there are certain areas of crime with a cross-border dimension which particularly require joint action within the EU to combat them. Article 83 TFEU makes provision for this.

Important rules have been laid down regarding the scope of such measures: firstly, the principle of subsidiarity limits the EU's right in principle to be more active in this area than in others. Secondly, the fundamental rights provided for in the European Convention on Human Rights and the Charter of Fundamental Rights require abstention from measures going beyond what is strictly necessary.

It should be noted to start with that the increased threat from terrorism and serious crime at the beginning of the last decade led to systems for the prevention of terrorism and serious crime being developed at European and international level. These systems continue to be effective.

The Stockholm Programme calls on the European Commission, on the basis of an impact assessment and while maintaining a high level of data protection, to present a proposal on the collection of PNR data. The Commission proposal under consideration provides for the retention of passenger data for a period of five years, irrespective of whether the passengers are suspected of anything, and the possibility of exchange of such data between Member States and with third countries. Since the value added that we may expect to derive from the proposed processing of PNR data as compared with that derived from existing instruments must be a determining factor for any provisions in this area, Austria has already been making efforts to obtain further empirical findings on the value added of an

EU PNR system. Such findings should above all serve to clarify whether the introduction of a binding, EU-wide PNR system is necessary at all.

There is clearly a certain tension between the proposal to store personal data of all air passengers on the scale proposed, irrespective of the existence of any specific suspicion, and the fundamental right to privacy and data protection (European Convention on Human Rights and Charter of Fundamental Rights). Implementation of such a measure could only be compliant with European and constitutional law if the measure is demonstrably necessary and proportionate. To evaluate whether this is the case, the strict criteria developed in the case law of the European Court of Human Rights and the Constitutional Court should be applied.

As it currently stands, the proposal for a Directive does not offer an adequate justification likely to stand the test of these criteria. The European Commission needs to provide still clearer evidence of the necessity and proportionality of such an intervention.

In general, an appropriate balance must be maintained in the fight against terrorism and serious crime between protection of fundamental rights and freedoms and protection of public safety. The Austrian Data Protection Council has adopted a unanimous position on the proposal for a Directive, which is annexed hereto."

Annex

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
(EU PNR Directive)

Position of the Data Protection Council

The **Data Protection Council** voted **unanimously at its 204th meeting on 28 February 2011** to adopt the following position on the above subject:

1. Background

On 2 February 2011 the Commission submitted a proposal for a Directive on the use of Passenger Name Record (PNR) data by the law enforcement authorities. This proposal follows on from earlier initiatives, the most recent of which was the Commission proposal for a Framework Decision introducing an EU PNR system (COM(2007)654).

The Data Protection Council has already **criticised and rejected** the proposal for a Framework Decision at its 180th meeting (5 March 2008) and 184th meeting (19 November 2008). It recommended to the Federal Ministries concerned (including the competent lead ministry, the Federal Ministry of the Interior) that they should oppose the initiative at EU level.

2. Key provisions

The provisions of the current proposal for a Directive, which in its essentials is similar to the proposed Framework Decision referred to above, may be summarised as follows:

1. Air carriers are to store the data of passengers on **international flights** into and out of Member States' territory (UK proposal: to be extended to intra-EU flights).

2. Air carriers are required to transfer these passenger data **24 hours before flight departure and immediately after flight closure** to the Passenger Information Unit to be established in each Member State (or jointly for more than one Member State).

3. These passenger data are to be retained at the national (or joint) Passenger Information Unit **in full for 30 days** and then **in "masked" form** (i.e. encrypted, with the key to the encryption retained at the national Passenger Information Unit) **for five years**.

4. The data are to be used for the prevention, detection, investigation and prosecution of **terrorist offences and serious crime** only (proposal from some MS: extend the scope of use).

5. Passenger data may be accessed only **shortly before, during or after the flight** to help locate persons being sought; at any later point within the five years the data may be accessed upon request by the authority/-ies of another State in order to search them for investigation or prosecution purposes (Article 4(2)(d) and Article 9(2) of the draft).

6. The data retained, and initially only "masked" (i.e. with personal details encrypted), may also be used for assessments in order to establish certain **patterns of behaviour** of typical suspects or groups of suspects and develop criteria with the help of which persons showing comparable patterns of behaviour can be subjected to a closer "screening" by the authorities. The Commission's impact assessment summarises these functions as follows: "*For example, an analysis of PNR data may give indications on the most usual travel routes for trafficking people or drugs which can be made part of assessment criteria. By checking PNR data in real-time against such criteria, crimes may be prevented or detected*."

3. Planned timing

The Commission is to present the proposal to the Council during the Justice and Home Affairs Council of 24 and 25 February 2011. Discussion of the content of the proposal by the Council's GENVAL Working Party is planned to commence as soon as 3 March 2011.

4. Austria's position so far

At EU level Austria (Federal Ministry of the Interior - BMI) has taken the position that a decentralised system (i.e. in which each Member State, or groups of Member States together, establish their own Passenger Information Unit) is not desirable and an EU-wide central PNR system would be preferable as it would provide greater "value added" (to summarise the position represented by the BMI most recently at the CATS meeting of 10 and 11 February 2011).

5. Data protection considerations regarding the proposed EU PNR system

5.1 General

Retaining the personal data of all air passengers, irrespective of any suspicion, is an invasion of privacy which, from the point of view of the fundamental right to respect for private life and data protection (Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights) is admissible only if it is provided for by law, is in the public interest and is absolutely necessary and proportional.

5.2. Suitability and necessity

If a legal act provides for such serious encroachments on fundamental rights, **the suitability and necessity thereof must be demonstrated in a concrete fashion.**

The present proposal supplements Directive 2004/82/EC, which already requires air carriers to transfer advance passenger information (API) for EU-bound flights to the national authorities responsible for improving border controls and combating illegal immigration.

However, the information content of PNR data goes far beyond that of API data. At the same time, the reliability of PNR data cannot be verified as they contain only the information which the person concerned supplied to the air carrier.

No specific empirical, objective data demonstrating the need for EU-wide use of these data (including retention for five years) for the purposes of public safety or their added value as compared with existing collections of data have yet been provided (cf. the comments of the European Data Protection Supervisor of 20 December 2007 and the Article 29 Group of 5 December 2007 http://ec.europa.eu/iustice/policies/privacy/docs/wpdocs/2007/wp145 de.pdf and most recently the position of the Article 29 Group on the Commission Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp178 de.pdf.)

In its position paper the Article 29 group repeatedly notes that even the pilot studies mentioned by the Commission do not justify the conclusion that the use of PNR data is necessary, efficient or proportional. Rather, it takes the view that the available information on instances of application point primarily to the use of API data rather than PNR data (see page 6 of the Article 29 position of 5 December 2007).

The - unsubstantiated - claim of the authorities that establishing such a State database creates "value added" for "monitoring" purposes is not, as it stands and without thorough examination of proportionality, a sufficient basis for the legal admissibility of an encroachment on fundamental rights.

Reference is sometimes also made to the fact that other States (UK, France, USA) already use PNR systems. However, in the absence of more detailed information on these systems, this is neither evidence that the measure is suitable and/or absolutely necessary for the whole EU, nor that these data retention and processing systems are compatible with our framework of fundamental rights (European Convention on Human Rights, Charter of Fundamental Rights).

It is also doubtful whether analysis of data based entirely on the statements of the person concerned is a suitable way of tracing criminals.

To summarise, the extremely brief **explanations given by the European Commission** in this proposal concerning the suitability or efficiency and necessity of such an EU PNR system **do not suffice to demonstrate** convincingly **either the fundamental suitability of the system nor the necessity** of the major encroachments on the fundamental right to data protection of countless (innocent) persons which the proposal entails.

5.3 Proportionality

5.3.1 Predictability of encroachment on fundamental rights

Like retention, all **further processing** (comparison, searches, linking, etc.) and also any passing on of these data, stored in a database, is a further serious intrusion into the private sphere of the persons concerned (including the innocent). It gives the State the possibility of investigating the lives of individuals by categorising or linking data without the knowledge of those concerned. These individual steps of processing would also be inadmissible in terms of fundamental and human rights unless necessary and proportional in the individual case.

As regards the **modus operandi of the European PNR system**, the draft does **not** specify **which data** (in real time) would be **compared** with which EU or national databases (and on the basis of what pre-defined "criteria" or risk analyses (Article 4(2)). Comparing all passenger data as part of risk analyses of citizens with no criminal record constitutes a huge intrusion into the private sphere of the individual. Such a comprehensive comparison of data, without prior legal provision for it, would be disproportionate and should be rejected on data

protection grounds. Moreover, any comparison of data **in accordance with certain "criteria" must be provided for by law**.

The fundamental right to respect for one's private life requires that State encroachments on the private sphere must be "provided for by law". This means that the person concerned must already be in a position to work out in advance, on the basis of the legal provisions, whether and in what ways his or her data will be processed by the State. Specific provision therefore needs to be made for this in the Directive, so that citizens can find out how and to what extent these data are used. **The Directive in the form currently proposed does not sufficiently meet these requirements.**

5.3.2 Retention by State authorities

The encroachment on a fundamental right is **all the more serious because** the data are retained (a) not by the air carrier itself, but by the State (b) for five years (cf. the shorter period in the Data Retention Directive) and (c) not only for the purpose of combating terrorism, but also for other purposes such as combating "serious" crime (see Article 2(h) and (i) of the draft Directive).

The seriousness of the encroachment in this case therefore substantially **exceeds the level** of that provided for in the Data Retention Directive (Directive 2006/24/EC), which itself already pushes at the limits of the admissible in terms of data protection law. The judgment of the Federal Constitutional Court on data retention expressly referred to the fact that the data retention only avoided being unconstitutional because the data were kept not by the State but by individual companies, no content data were recorded and the retention period provided for was only six months (Federal Constitutional Court 2.3.2010, 1 BvR 256/08 and others).

Against this background, the **admissibility of State collection of flight data** seems **doubtful in the light of the limits set by fundamental rights**. It should be pointed out that issues relating to fundamental rights are not least amongst those informing the European Commission's ongoing evaluation of the Data Retention Directive.

5.3.3. Duration of data retention

Under the current proposal the passenger data would be retained at the national (or joint) Passenger Information Unit in full for 30 days and then in "masked" form (i.e. encrypted, with the key to the encryption retained at the national Passenger Information Unit) for five years.

The masking out provided for in Article 9 is intended - at least provisionally - to eliminate the identifying data. However, the categories of data to be masked out under Article 9(2) do not appear to be sufficient, particularly since the data listed under points 6 or 8 of the Annex would apparently be retained and so the possibility of identifying the person would not be eliminated.

In the light of the above references to the Data Retention Directive and in the absence of evidence of necessity, **such a long retention period appears disproportionate**.

5.3.4 Preventive and independent monitoring

Under ECHR case law, an arrangement allowing for retention and access over a five-year period is in any case inadmissible if the rules fail to guarantee appropriate and **effective monitoring** of every individual case to prevent abuse (ECHR case *Rotaru* v *Romania*, 28341/95, § 59 with further references). The principle of the rule of law requires *inter alia* that any given encroachment by the authorities on the rights of the person concerned (file search, data linking etc.) **is subject to an effective control mechanism**, generally operated by the **Courts or an independent body** (see ECHR in case *Rotaru* v *Romania*, 28341/95, § 59, and case *Klass* v *Germany* 6.9.1978, § 55).

Furthermore, the fact that, for practical reasons or on the grounds of investigative tactics, the person concerned cannot be informed of the intervention cannot be used as an argument against such mechanisms. Member States' legal systems afford many examples of control mechanisms specifically aimed at the kind of investigative measure which cannot initially be notified to the person concerned. One may cite as examples prior checks by judges before phone tapping or computer-assisted dragnet searches are allowed, or institutions such as a citizens' rights ombudsman who has the power to authorise data searches in advance and seek legal remedy to protect the person concerned.

In the light of the fundamental right to respect of private life (Article 8 ECHR) such independent monitoring of individual cases is **essential**.

The interposition of an effective and independent control mechanism is thus called for in connection with both national authorities' access to data (Article 4(2)(c) in conjunction with Article 2 of the proposal) and access resulting from enquiries or transmission to (an)other

State(s) under Article 7 of the proposal (e.g. monitoring by an independent ombudsman or supervisory authority).

To summarise, the present draft Directive **does not provide any basis for independent prior checks** on encroachments on fundamental rights. The encroachments on fundamental rights provided for in the draft Directive are also lacking in proportionality because the **control mechanisms and mechanism for the protection of rights** provided for in the draft do **not** appear to be **independent or effective**.

6. Conclusions

The plan to introduce an EU PNR system as set out in the Commission proposal must be **assessed critically** in terms of data protection. Since under EU law it has hitherto been up to the Member States to decide whether to maintain a PNR system, it is not clear why it is now considered necessary to introduce such systems, associated with major encroachments on fundamental rights, by means of a Directive binding on all Member States (subsidiarity).

During EU negotiations the **competent lead service** should ensure that comprehensive **explanations concerning the suitability and necessity** of the EU PNR system are provided. Austria should also make efforts to ensure that **proportionate solutions are found** regarding the predictability of encroachments on fundamental rights, the retention of the data by the State and the length of the retention period. **Control mechanisms** guaranteeing independent and effective monitoring of the authorities' use of the data must be added to the proposal.

If additional explanations of the suitability and necessity of the measures, and provisions guaranteeing proportionality **cannot be obtained and the issue of costs cannot be resolved**, it is again recommended (cf. earlier positions of the Data Protection Council of 11.3.2008, ref BKA-817.324/0002-DSR/2008, and of 28.11.2008, ref 817.324/0005-DSR/2008) that the competent lead service should **oppose this initiative** at EU level.