A data protection critique of the proposed Passenger Name Record Directive

(*COM(2011) 32 text*)

A DATA PROTECTION ANALYSIS
FROM AMBERHAWK TRAINING LTD
DR. C. N. M. POUNDER, JUNE 2011

EUROPEAN COMMISSION

Brussels, 2.2.2011

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**

(Recitals removed)

CHAPTER I

GENERAL PROVISIONS

Article 1: **Subject matter and scope**

1. This Directive provides for the transfer by air carriers of Passenger Name Record data of passengers of international flights to and from the Member States, as well as the processing of that data, including its collection, use and retention by the Member States and its exchange between them.

2. The PNR data collected in accordance with this Directive may be processed only for the following purposes:

(a) The prevention, detection, investigation and prosecution of terrorist offences and serious crime according to Article 4(2)(b) and (c); and

(b) The prevention, detection, investigation and prosecution of terrorist offences and serious transnational crime according to Article 4(2)(a) and (d).

Article 2

Definitions

For the purposes of this Directive the following definitions shall apply:

(a) 'air carrier' means an air transport undertaking with a valid operating licence or equivalent permitting it to carry out carriage by air of passengers;

(b) 'international flight' means any scheduled or non-scheduled flight by an air carrier planned to land on the territory of a Member State originating in a third country or to depart from the territory of a Member State with a final destination in a third country, including in both cases any transfer or transit flights;

Comment [U1]: This definition and Article 1 needs changing if the provision is to apply to internal EEA flights.

(c) 'Passenger Name Record' or 'PNR data' means a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey

booked by or on behalf of any person, whether it is contained in reservation systems, Departure Control Systems (DCS) or equivalent systems providing the same functionalities;

(d) 'passenger' means any person, except members of the crew, carried or to be carried in an aircraft with the consent of the carrier;

(e) 'reservation systems' means the air carrier's internal inventory system, in which PNR data are collected for the handling of reservations;

(f) 'push method' means the method whereby air carriers transfer the required PNR data into the database of the authority requesting them;

(g) 'terrorist offences' means the offences under national law referred to in Articles 1 to 4 of Council Framework Decision 2002/475/JHA;

[***The problem is that this is a wide definition- as is explained in the margin***]

(h) 'serious crime' means the offences under national law referred to in Article 2(2) of Council Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State, however, Member States may exclude those minor offences for which, taking into account their respective criminal justice system, the processing of PNR data pursuant to this directive would not be in line with the principle of proportionality;

(i) 'serious transnational crime' means the offences under national law referred to in Article 2(2) of Council Framework Decision 2002/584/JHA if they are punishable by a custodial sentence or a detention order for a maximum period of at least three years under the national law of a Member State, and if :

(i) They are committed in more than one state;

(ii) They are committed in one state but a substantial part of their preparation, planning, direction or control takes place in another state;

(iii) They are committed in one state but involve an organised criminal group that engages in criminal activities in more than one state; or

(iv) They are committed in one state but have substantial effects in another state.

Comment [U2]: What is a "serious crime"? It often the case that "serious" might not be that serious.

Comment [U3]: There is a drafting issue here. If a "law of a Member State" has a three year penalty for crime X, then a Member State that does not have a 3 year penalty for the same crime X can still transmit PNR data

The 3 year penalty relates to a penalty established by **ANY** Member State and **NOT NECESSARILY** the Member State to which (or from which) the passenger is travelling. This definition ensures that there is an Euro-wide "**lowest common denominator"** definition of "serious crime" is used.

There are many problems in the UK re European Arrest Warrants which uses the "serious crime" test. The use of this definition could well exacerbate those problems if the Directive applies internally (examples of serious crime given in the Hawktalk blog of 8th Feb 2011 are not serious crimes – indeed, some appear to be more like disputes such as not paying a bill for a meal because it was awful).

Comment [U4]: The "may" here could mean "may not" (i.e. include); there is no obligation to exclude minor "serious crime". The fact that this "may" is not a "must" means that the scope of the crimes the Directive covers is subject to wide discretion by a Member State. I can't see why "may" is being used instead of "must" unless the intention is to transfer as many crimes as a Member State can transfer.

Another improvement would be if the likely punishment (if there were to be a guilty verdict) has to be more than 3 years in prison. This gets round the problem of a statute providing for an offence of a maximum 3 year sentence but in practice it is very unlikely that this would be the actual punishment (if someone was found guilty).

Alternatively, you could say a maximum of three years penalty has to occur "i**n the majority or two thirds of Member States".**

Comment [U5]: The EDPS wants "Minor crime" to be defined. If it could be defined, then those crimes that are **not** minor crimes could be the ones subject to the Directive.

This is an attractive alternative proposition if possible: "This Directive does not apply to minor crimes" where a "minor crime is ....." (if it can be done)

CHAPTER II

RESPONSIBILITES OF THE MEMBER STATES

Article 3: **Passenger Information Unit [*Article 3(2) is suspect*]**

1. Each Member State shall set up or designate an authority competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime or a branch of such an authority to act as its 'Passenger Information Unit' responsible for collecting PNR data from the air carriers, storing them, analysing them and transmitting the result of the analysis to the competent authorities referred to in Article 5. Its staff members may be seconded from competent public authorities.

2. Two or more Member States may establish or designate a single authority to serve as their Passenger Information Unit. Such Passenger Information Unit shall be established in one of the participating Member States and shall be considered the national Passenger Information Unit of all such participating Member States. The participating Member States shall agree on the detailed rules for the operation of the Passenger Information Unit and shall respect the requirements laid down in this Directive.

[ARTICLE 3(2) CAN *UNDERMINE* THE PROTECTIVE ELEMENTS OF THE DIRECTIVE]

This prospect arises because of the use of the phrase "***the*** national Passenger Information Unit of all such participating Member States". Suppose Member States A, B and C merge their PIUs – the use of the word "***the***" means there is now only ***ONE*** PIU for these three States. Thus the concept of transfer between PIUs does not exist if there is only ***ONE*** PIU; therefore the "safeguards" with respect to such transfers do not exist.

This provision therefore encourages the development of a mega PIU and merged Euro mega-database (despite contrary comments from the relevant Commissioner). A merger of PIUs should be regarded as a likely outcome. The fact that Member States have to show "respect" to the Directive is not a safeguard; it means that the PIU can effectively make up its own procedures that "roughly" meet the obligations in this Directive. **This provision should at the very least ensure that each merged PIU of the Member State still has legal status following any merging of PIUs**].

3. Each Member State shall notify the Commission thereof within one month of the establishment of the Passenger Information Unit and may at any time update its declaration. The Commission shall publish this information, including any updates, in the *Official Journal of the European Union.*

Article 4: **Processing of PNR data**

1. The PNR data transferred by the air carriers, pursuant to Article 6, in relation to international flights which land on or depart from the territory of each Member State shall be collected by the Passenger Information Unit of the relevant Member State. Should the PNR data transferred by air carriers include data beyond those listed in the

Comment [U6]: Only one PIU per member state, but note a PIU could be part ("a branch") of a competent authority (i.e. "an authority competent for the prevention of crime" etc).

In other words the PIU is not the independent body that it appears to be.

Comment [U7]: In addition, following on from the above comment, if the PIU is staffed with people from a competent authority then they are very likely to make decisions in favour of disclosure to that competent authority. This should not surprise anyone.

So when tests such as assessing on "a case-by-case basis, to duly reasoned requests" as in Article 4(2)(c) are undertaken, a likely outcome of that assessment will be a decision in favour of disclosure (especially if the person doing the assessment is a seconded member of staff of that competent authority!)

As I explain below, there needs to be a threshold test where transfer to a competent authority should occur when failure to transfer would prejudice an actual criminal inquiry.

Comment [U8]:

THIS PROVISION CAN UNDERMINE THE PROTECTIVE ELEMENTS OF THE PNR DIRECTIVE (as is explained in the text at the side).

Each PIU, in my view has to have a legal identity (I am not sure it will have a legal identity if it is a branch of a competent authority (see U6 and U7 above) – otherwise you will have an incentive to form mega PIU's developing.

Comment [U9]: There is no penalty if a Member State does not notify the existence of the PIU to the Commission. In Data Protection terms the UK has a bad record in failing to notify the Commission (e.g. the additional uses of sensitive personal data ; see Hawktalk blog of 14/02/2011).

One minor improvement is to say the PIU cannot process PNR data unless the Member State notifies. This will force notification. The PIU information published should also include contact details so the public can exercise their rights.

Annex, the Passenger Information Unit shall delete such data immediately upon receipt.

2. The Passenger Information Unit shall process PNR data only for the following purposes:

(a) carrying out an assessment of the passengers prior to their scheduled arrival or departure from the Member State in order to identify any persons who may be involved in a terrorist offence or serious transnational crime and who require further examination by the competent authorities referred to in Article 5. In carrying out such an assessment, the Passenger Information Unit may process PNR data against pre-determined criteria. Member States shall ensure that any positive match resulting from such automated processing is individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action;

(b) carrying out an assessment of the passengers prior to their scheduled arrival or departure from the Member State in order to identify any persons who may be involved in a terrorist offence or serious crime and who require further examination by the competent authorities referred to in Article 5. In carrying out such an assessment the Passenger Information Unit may compare PNR data against relevant databases, including international or national databases or national mirrors of Union databases, where they are established on the basis of Union law, on persons or objects sought or under alert, in accordance with Union, international and national rules applicable to such files. Member States shall ensure that any positive match resulting from such automated processing is individually reviewed by non-automated means in order to verify whether the competent authority referred to in Article 5 needs to take action;

(c) responding, on a case-by-case basis, to duly reasoned requests from competent authorities to provide PNR data and process PNR data in specific cases for the purpose of prevention, detection, investigation and prosecution of a terrorist offence or serious crime, and to provide the competent authorities with the results of such processing; and

(d) analysing PNR data for the purpose of updating or creating new criteria for carrying out assessments in order to identify any persons who may be involved in a terrorist offence or serious transnational crime pursuant to point (a).

3. The assessment of the passengers prior to their scheduled arrival or departure from the Member State referred to in point (a) of paragraph 2 shall be carried out in a non discriminatory manner on the basis of assessment criteria established by its Passenger Information Unit. Member States shall ensure that the assessment criteria are set by the Passenger Information Units, in cooperation with the competent authorities referred to in Article 5. The assessment criteria shall in no circumstances be based on a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life.

4. The Passenger Information Unit of a Member State shall transfer the PNR data or the results of the processing of PNR data of the persons identified in accordance with points (a) and (b) of paragraph 2 for further examination to the relevant competent authorities of the same Member State. Such transfers shall only be made on a case by-case basis.

Comment [U10]: Article 2(a) and 2(d) do not apply to "serious crime"; only terrorism and serious transnational crime.

Comment [U11]: Note that "Serious transnational crime" and "terrorist offences" are a very small subset of the totality of ALL "serious crime".

This explains why the PNR Directive has to be judged in a context that does not focused on terrorism or serious transnational crime; the Directive is primarily about "serious crime" that is not serious transnational or not terrorist related.

That is why the definition of serious crime is **ALL** important (see comment at U2-U5).

Comment [U12]: See U11 above

Comment [U13]: The use of the plural "criteria" instead of "criterion" confuses what is intended. I am not sure whether this prohibition applies if ONE of the many criteria used to make an assessment is for example, "race" or "religion". The use of "assessment criteria" means, I think, that ALL the assessment criteria taken as a whole cannot be based on race, religion etc.

This kind of drafting discrepancy can result in diverse implementations of the Directive by Member States I therefore think a amendment replacing the above with a provision that uses the singular is needed: for example "Any assessment criterion shall in no circumstances...."

Comment [U14]: Although the PIU considers transfers on a case-by-case (and is in a position keep decent records or statistics on transfers), the Member State is not under an obligation to report statistics on these transfers. (This is very relevant as the reporting of statistics provisions are particularly poor – see A.18).

Article 5: **Competent authorities**

[A lower level of data protection is guaranteed by Article 5; see commentary re Article 6 which explains this fully. This is a particularly weak provision as there is an absence of safeguards and transparency as explained in the margins of this Article and Article 6. The list provisions of this Article are especially weak and there is no provision relating to onward disclosure of PNR data by competent authorities to bodies that are not competent authorities.

The PNR Directive excludes reference to the national security agencies; the extent to which PNR data are processed by these agencies is also absent in the Directive. One has to assume that this is deliberate. As national security agencies are likely to have generous powers to process PNR data and can take advantage of the normally broad exemptions found in national laws for national security purposes, one can anticipate that these agencies could hold copies of all PNR data for more than the 5 year period. If this is the case, then retention periods specified in the Directive are rendered meaningless, as some competent authorities can always recover PNR data from national security sources.]

1. Each Member State shall adopt a list of the competent authorities entitled to request or receive PNR data or the result of the processing of PNR data from the Passenger Information Units in order to examine that information further or take appropriate action for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime.

2. Competent authorities shall consist of authorities competent for the prevention, detection, investigation or prosecution of terrorist offences and serious crime.

3. Each Member State shall notify the list of its competent authorities to the Commission twelve months after entry into force of this Directive at the latest, and may at any time update its declaration. The Commission shall publish this information, as well as any updates, in the *Official Journal of the European Union*.

4. The PNR data of passengers and the result of the processing of PNR data received by the Passenger Information Unit may be further processed by the competent authorities of the Member States only for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious crime.

5. Paragraph 4 shall be without prejudice to national law enforcement or judicial powers where other offences, or indications thereof, are detected in the course of enforcement action further to such processing.

6. The competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data. Such decisions shall not be taken on the basis of a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life.

[***An amendment is needed to this Article on the lines: "A competent authority can only disclose PNR data to other competent authorities". Also there is no obligation placed on competent authorities to keep statistics of their use or disclosure of PNR data nor is there any restriction on any onward disclosures made to other bodies in the Member State of the competent authority that gets the PNR data.***

Comment [U15]: There are no data protection obligations placed on competent authorities by this Directive. At least, one would expect to see a reference to the application of the low data protection standards of Framework Decision 2008/977/JHA applying to each competent authority. (The absence of a reference could be because of national security but if this is the case, this should be explicit exemption for national security so that Parliamentarians can debate the exemption)

Note that the Directive does not empower the data protection supervisory authority to audit a competent authority as appropriate as a means of engaging the data protection authority with DP compliance by a competent authority.

Comment [U16]: . What is notified to the Commission could contain little detail (e.g. in the UK there are 40+ police forces – the list could be limited to two words ("the police"). Or it might identify each police force. Who knows? ***An improvement in transparency is needed and the notification requirements need to be standardised.***

The plural "its competent authorities" should be changed to the singular "***each*** competent authority" so to ensure that ***all*** competent authorities are identified.

Comment [U17]: There is no penalty on a Member State if competent authorities are not notified. I would also specify that name and contact address so that individuals can make contact with respect of their rights.. The provision leaves the list's content to the whim of a Member State.

The data protection authorities (e.g. possibly via WP29) should determine what is notified and listed.

Comment [U18]: Note there is no restriction on competent authorities if they chose to forward the PNR data to other bodies, within a Member State, who are not competent authorities. That is why the amendment below is important

Suggest an amendment that states that "any body that receives PNR data has to be a competent authority" will identify all bodies that get PNR data. Onward data sharing needs to be addressed when this Directive is debated.

Comment [U19]: This provision requires the computer to make the assessment - "**only** by reason of automated processing". So it is possible for a computer to "suggest" a decision and ask a human operator to confirm it. This use of the word "only" limits the protection afforded by this provision

Comment [U20]: Directive does not provide for a penalty if competent authorities ignore this provision. Data protection authorities should be given powers to enforce this provision, or should be able to audit a competent authority.

Article 6 **Obligations on air carriers**

Comment [U21]: See the yellow at the side as it **helps explain why Article 8 is so poor.**

This provision in Article 6 should be read in conjunction with Articles 5 and 8 as it provides a contrast between the levels of protection afforded by air carriers and PIUs and Competent Authorities. Articles 5, 6 and 8 provide for minimal data protection.

In summary, air carriers when processing PNR data are subject to the higher standards of Directive 95/46/EC. Yet when the same personal data are in the hands of PIUs and Competent Authorities one assumes that the lower standards of Framework Decision 2008/977/JHA apply (**Note** the word "assumes": I am really not sure the Framework does apply to all organisations that will obtain PNR data. This needs probing).

The Commission is therefore proposing the transfer of the same personal data that have a high level of protection in the hands of the air carrier to the lower level of protection in the hands of organisations that involved in law enforcement. This standard becomes even lower, if you consider the prospect of allowed transfers of PNR data to Third Countries (see Article 8).

The result is that a lower standard of Data Protection applies when the purpose is more controversial (e.g. associated with arrest etc). This is an "***inverse" data protection effect.*** The more controversial the purpose (e.g.law enforcement) the lower the level of data protection; the less controversial the purpose (e.g. processing a seat booking), the higher the level of data protection.

Comment [U22]: I think this explains why the Europoean Data Protection supervisor has come to the same conclusion.

Directive 95/46/EC should apply – it is really a nonsense that it doesn't

[Suggested *amendment is that "the level of data protection applicable to PNR data processed by a competent authority and a Passenger Information Unit is that specified in Directive 95/46/EC"*]

1. Member States shall adopt the necessary measures to ensure that air carriers transfer ('push') the PNR data as defined in Article 2 (c) and specified in the Annex, to the extent that such data are already collected by them, to the database of the national Passenger Information Unit of the Member State on the territory of which the international flight will land or from the territory of which the flight will depart. Where the flight is code-shared between one or more air carriers, the obligation to transfer the PNR data of all passengers on the flight shall be on the air carrier that operates the flight. Where the flight has one or more stop-overs at the airports of the Member States, air carriers shall transfer the PNR data to the Passenger Information Units of all the Member States concerned.

2. Air carriers shall transfer PNR data by electronic means using the common protocols and supported data formats to be adopted in accordance with the procedure of Articles 13 and 14 or, in the event of technical failure, by any other appropriate means ensuring an appropriate level of data security:

(a) 24 to 48 hours before the scheduled time for flight departure; and

(b) immediately after flight closure, that is once the passengers have boarded the aircraft in preparation for departure and it is no longer possible for further passengers to board.

3. Member States may permit air carriers to limit the transfer referred to in point (b) of paragraph 2 to updates of the transfer referred to in point (a) of paragraph 2.

4. On a case-by-case basis, upon request from a Passenger Information Unit in accordance with national law, air carriers shall transfer PNR data where access earlier than that mentioned in point (a) of paragraph 2 is necessary to assist in responding to a specific and actual threat related to terrorist offences or serious crime.

Article 7: **Exchange of information between Member States**

1. Member States shall ensure that, with regard to persons identified by a Passenger Information Unit in accordance with Article 4 (2)(a) and (b), the result of the processing of PNR data is transmitted by that Passenger Information Unit to the Passenger Information Units of other Member States where the former Passenger Information Unit considers such transfer to be necessary for the prevention, detection, investigation or prosecution of terrorist offences or serious crime. The Passenger Information Units of the receiving Member States shall transmit such PNR data or the result of the processing of PNR data to their relevant competent authorities.

2. The Passenger Information Unit of a Member State shall have the right to request, if necessary, the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database in accordance with Article 9(1), and, if necessary, also the result of the processing of PNR data. The request for such data may be based on any one or a combination of data elements, as deemed necessary by the requesting Passenger Information Unit for a specific case of prevention, detection, investigation or prosecution of terrorist offences or serious crime. Passenger Information Units shall provide the requested data as soon as practicable and shall provide also the result of the processing of PNR data, if it has already been prepared pursuant to Article 4(2)(a) and (b).

3. The Passenger Information Unit of a Member State shall have the right to request, if necessary, the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database in accordance with Article 9(2), and, if necessary, also the result of the processing of PNR data. The Passenger Information Unit may request access to specific PNR data kept by the Passenger Information Unit of another Member State in their full form without the masking out only in exceptional circumstances in response to a specific threat or a specific investigation or prosecution related to terrorist offences or serious crime.

4. Only in those cases where it is necessary for the prevention of an immediate and serious threat to public security may the competent authorities of a Member State request directly the Passenger Information Unit of any other Member State to provide it with PNR data that are kept in the latter's database in accordance with Article 9(1) and (2). Such requests shall relate to a specific investigation or prosecution of terrorist offences or serious crime and shall be reasoned. Passenger Information Units shall respond to such requests as a matter of priority. In all other cases the competent authorities shall channel their requests through the Passenger Information Unit of their own Member State.

5. Exceptionally, where early access is necessary to respond to a specific and actual threat related to terrorist offences or serious crime, the Passenger Information Unit of a Member

Comment [U23]: I shall use the use of "shall" here to illustrate an interpretation point which occurs often when reading this Directive. It might help the reader to appreciate the consequences of small word changes.

"Shall" means that the request cannot be refused; its use provides an example that the Directive wants something to happen in **ALL** Member States. Hence the use of words like "shall" or "must" in the text of Articles.

By inference, therefore, when the text uses the word "may" (e.g. see definition of "serious crime" for example), it means the provision ***might not*** apply.

This provides flexibility to Member States to make their own provision. Some "**may**" do something whilst other States "**may not**". In other words, the use of the word "may" often means that there is a likely divergence between Member States as to the implementation of this Directive.

See U2-U5 on the "may" used in relation to the inclusion of "serious crime" or the "may" as used in U25 for example.

Comment [U24]: A request "**may**" be based on these data elements, but then of course it "**may not**". One wonders whether the "may" here should be replaced by "must" and a threshold test that failure to disclose would prejudice serious crime.

This threshold test can be (and should be) applied in several areas of this Directive

Comment [U25]: "Deemed" necessary - is not the strict test of "necessity" required by Article 8(2) of the Human Rights Convention in relation to interference. The test where "necessity" here is qualified by "deemed".

Remember the individual doing the "deeming" in the PIU might be an employee of the competent authority making the request (or the PIU might even be part of the competent authority) (see A.3(1)). Hence there is no prize for identifying the outcome of any "deeming".

I would be surprised if a PIU comprising of law enforcement officers brought up in a law enforcement culture do not deem most requests as being necessary!

Comment [U26]: It is very easy to insert a higher threshold test here in all these exchanges between Member States.

For example one could easily have a threshold obligation here that the PIU has to be satisfied that "failure to disclose would prejudice a specific case of serious crime". (This is the test used by the UK's DPA).

State shall have the right to request the Passenger Information Unit of another Member State to provide it with PNR data of flights landing in or departing from the latter's territory at any time.

6. Exchange of information under this Article may take place using any existing channels for international law enforcement cooperation. The language used for the request and the exchange of information shall be the one applicable to the channel used. Member States shall, when making their notifications in accordance with Article 3(3), also inform the Commission with details of the contacts to which requests may be sent in cases of urgency. The Commission shall communicate to the Member States the notifications received.

Article 8: **Transfer of data to third countries –**

This Article applies Council Framework Decision 2008/977/JHA **ONLY** to the **TRANSFER** (i.e. **It does not even state** that the Decision applies to **all** competent authorities or PIUs). In addition, there is hardly any provision in this Article or Directive that ensures transparency of such transfers as is explained in the marginal comments.

A Member State may transfer PNR data and the results of the processing of PNR data to a third country, only on a case-by-case basis and if:

(a) the conditions laid down in Article 13 of Council Framework Decision 2008/977/JHA are fulfilled

(b) the transfer is necessary for the purposes of this Directive specified in Article 1(2), and

(c) the third country agrees to transfer the data to another third country only where it is necessary for the purposes of this Directive specified in Article 1(2) and only with the express authorisation of the Member State.

Article 9: **Period of data retention**

[***The retention period provisions use the word "anonymised" in a way that means that the individual is not anonymous. The PNR data are personal data despite the "anonymisation" process identified in this Article. If the Commission continue the use of "anonymised" in this way, it not only is it totally misleading, it is also ridiculous.***]

1. Member States shall ensure that the PNR data provided by the air carriers to the Passenger Information Unit are retained in a database at the Passenger Information Unit for a period of 30 days after their transfer to the Passenger Information Unit of the first Member State on whose territory the international flight is landing or departing.

Comment [U27]: MUST SEE COMMENTARY RE ARTICLE 19 AND THE APPENDIX WHICH LISTS DECISION 2008/977/JHA.

There is a risk that data protection considerations play no part in a transfer and there is little role for the data protection authority in the transfer.

Comment [U28]: If the words "Member State" were changed to "competent authority", this would reduce the risk that Member State could arrange transfers for political reasons (see Appendix for explanation of this).

A competent authority would be more likely to transfer for functional reasons (e.g. very serious crime, terrorism). However, there is still the problem that PNR data are no longer subject to data protection safeguards based on Directive 95/46/EC

Comment [U29]: Note that you might get one Member State transferring in circumstances where other States do not.

Comment [U30]: In effect Member States can more or less go their own way on this and could permit transfers in circumstances where a PIU would not transfer from within Europe

Comment [U31]: This includes serious crime in the Third Country. Depends much on the Third Country – some offences (e.g. re homosexuality) are not offences in the EU. This provision also allows exchanges of information with **ANY** Third Country. There is little involvement of a data protection supervisory authority.

Comment [U32]: Amendments to limit the scope of these transfers is to restrict the offences to terrorist and serious international crime by changing "1(2)" to "1(2) excluding the provisions relating to serious crime".

Or you could define "very serious crime" for this provision where very serious crime could be a 6 year sentence in BOTH the Member State and the Third Country (and any forwarding third country).

Comment [U33]: There is no penalty if transfer to third countries occurs without authorisation. Member States are very likely to authorise especially if there is no transparency. I suggest that details of such authorisations should be notified to the Commission or data protection authorities.

Finally, there is no obligation to keep records of these transfers which can be reported. I think this is a shocking omission – if it is deliberate.

2. Upon expiry of the period of 30 days after the transfer of the PNR data to the Passenger Information Unit referred to in paragraph 1, the data shall be retained at the Passenger Information Unit for a further period of five years. During this period, all data elements which could serve to identify the passenger to whom PNR data relate shall be masked out. Such anonymised PNR data shall be accessible only to a limited number of personnel of the Passenger Information Unit specifically authorised to carry out analysis of PNR data and develop assessment criteria according to Article 4(2)(d). Access to the full PNR data shall be permitted only by the Head of the Passenger Information Unit for the purposes of Article 4(2)(c) and where it could be reasonably believed that it is necessary to carry out an investigation and in response to a specific and actual threat or risk or a specific investigation or prosecution. For the purposes of this Directive, the data elements which could serve to identify the passenger to whom PNR data relate and which should be filtered and masked out are: – Name (s), including the names of other passengers on PNR and number of travellers on PNR travelling together; – Address and contact information; – General remarks to the extent that it contains any information which could serve to identify the passenger to whom PNR relate; and – Any collected Advance Passenger Information.

3. Member States shall ensure that the PNR data are deleted upon expiry of the period specified in paragraph 2. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific criminal investigations or prosecutions, in which case the retention of such data by the competent authority shall be regulated by the national law of the Member State.

4. The result of matching referred to in Article 4(2)(a) and (b) shall be kept by the Passenger Information Unit only as long as necessary to inform the competent authorities of a positive match. Where the result of an automated matching operation has, further to individual review by non-automated means, proven to be negative, it shall, however, be stored so as to avoid future 'false' positive matches for a maximum period of three years unless the underlying data have not yet been deleted in accordance with paragraph 3 at the expiry of the five years, in which case the log shall be kept until the underlying data are deleted.

Article 10: **Penalties against air carriers**

Member States shall ensure, in conformity with their national law, that dissuasive, effective and proportionate penalties, including financial penalties, are provided for against air carriers which, do not transmit the data required under this Directive, to the extent that they are already collected by the them, or do not do so in the required format or otherwise infringe the national provisions adopted pursuant to this Directive.

Article 11: **Protection of personal data**

(***Suggested amendment*:** in the above put **"*A much lower level of*"** before the word **"*Protection*".** In addition the transparency (listing) provisions are very inadequate

1. Each Member State shall provide that, in respect of all processing of personal data pursuant to this Directive, every passenger shall have the same right to access, the right to rectification, erasure and blocking, the right to compensation and the right to judicial redress as those adopted under national law in implementation of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA. The provisions of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA shall therefore be applicable.

Comment [U34]: These anonymised data are still personal data in the hands of the PIU. The data are not anonymised at all. The use of "anonymised" is simply misleading.

The EDPS says it should be deleted unless there is a reason for retention.

Comment [U35]: I would put in an amendment to establish a threshold test (e.g. failure to disclose would prejudice a specific criminal investigation").

At the moment the Head of the PIU has to reasonably believe; this is not a high threshold at all. This is especially the case if the Head of the PIU is seconded from a competent authority, or if the PIU is part of the competent authority.

Comment [U36]: Is this the 5 year period.

Comment [U37]: If the air carriers get it wrong – dissuasive penalties. If the PIU or competent authorities get it wrong – no dissuasive penalties.

This shows the Directive is not balanced

Comment [U38]: This is the right of access to personal data that passengers have provided – so it does not add up to much, assuming passengers can remember which flight they were on and where they were going.

I suggest an amendment that expressly states that this includes any log of disclosure relating to passenger data in circumstances where there is no prejudice to the purposes identified in Article 1(2).

Comment [U39]: To exercise a right of judicial redress, the aggrieved passenger has to take on the State. This is a very difficult ask.

Comment [U40]: There is a drafting issue here as the current text states explicitly that only Articles 17 to 20 of the Council Framework Decision 2008/977/JHA are applicable. By inference other Articles of the Decision may not be applicable.

If the provision said "In particular, the provisions of Articles 17, 18, 19 and 20 of the Council Framework Decision 2008/977/JHA shall therefore be applicable" then this problem would not occur.

Directive 95/46/EC **fully applies to PNR data when in the hands of the airlines**; this provision thus ensures a lower level of protection proffered by Council Framework Decision 2008/977/JHA

2. Each Member State shall provide that the provisions adopted under national law in implementation of Articles 21 and 22 of the Council Framework Decision 2008/977/JHA regarding confidentiality of processing and data security shall also apply to all processing of personal data pursuant to this Directive

3. Any processing of PNR data revealing a person's race or ethnic origin, religious or philosophical belief, political opinion, trade union membership, health or sexual life shall be prohibited. In the event that PNR data revealing such information are received by the Passenger Information Unit they shall be deleted immediately.

[The comments about logs in the margin are very important, as they will result in meaningless information which will not allow independent assessment of whether or not the PNR Directive is of any value. This very weak drafting is deliberate.

On 31st May, the EDPS published an opinion on the European Commission's evaluation report on the Data Protection Directive (2006/24/EC). He criticised the statistics collected by Member States to justify the retention of telecommunciations data. He says "Although the Commission has clearly put much effort into collecting information from the Member States, the quantitative and qualitative information provided by the Member States is not sufficient to draw a positive conclusion on the need for data retention as it has been developed in the Directive"

The provisions below are designed to ensure that such quantitative and qualitative information that could justify the PNR Directive are not collected.]

4. All processing of PNR data by air carriers, all transfers of PNR data by Passenger Information Units and all requests by competent authorities or Passenger Information Units of other Member States and third countries, even if refused, shall be logged or documented by the Passenger Information Unit and the competent authorities for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security of data processing, in particular by the national data protection supervisory authorities. These logs shall be kept for a period of five years unless the underlying data have not yet been deleted in accordance with Article 9(3) at the expiry of those five years, in which case the logs shall be kept until the underlying data are deleted.

Comment [U41]: The content of logs are too important to be left unspecified and at the whim of Member States law enforcement community (see next comment)

Comment [U42]: I suggest that as the content of the logs that relate to data protection matters and any retention criteria should be specified by the national supervisory data protection authority or in consultation with the EDPS/WP29. These authorities should also empowered to require certain statistics to be collected. This will ensure that an independent cost-benefit analysis performed – not the in-house analysis undertaken by the Commission.

If this change is not made then the logs will be meaningless. Member States might only log those things that support the PNR data processing.

Note that Articles 17 and 18 provide for reviews and statistics that are not independent of the Commission or Member States who could easily arrange the statistical data collection to show how the system is working well!

VERY IMPORTANT IN MY VIEW.

5. Member States shall ensure that air carriers, their agents or other ticket sellers for the carriage of passengers on air service inform passengers of international flights at the time of booking a flight and at the time of purchase of a ticket in a clear and precise manner about the provision of PNR data to the Passenger Information Unit, the purposes of their processing, the period of data retention, their possible use to prevent, detect, investigate or prosecute terrorist offences and serious crime, the possibility of exchanging and sharing such data and their data protection rights, in particular the right to complain to a national data protection supervisory authority of their choice. The same information shall be made available by the Member States to the public.

6. Any transfer of PNR data by Passenger Information Units and competent authorities to private parties in Member States or in third countries shall be prohibited.

7. Without prejudice to Article 10, Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down

effective, proportionate and dissuasive penalties to be imposed in case of infringements of the provisions adopted pursuant to this Directive.

Article 12: **National supervisory authority**

[This provision is designed to allow some Member States to exclude the data protection authority from certain aspects of the processing of PNR data. The PNR Directive sets out to promote fragmentation of the regime that protects the public from misuse of PNR data but unifies the organisations that process the PNR data.]

Each Member State shall provide that the national supervisory authority established in implementation of Article 25 of Framework Decision 2008/977/JHA shall also be responsible for advising on and monitoring the application within its territory of the provisions adopted by the Member States pursuant to the present Directive. The further provisions of Article 25 Framework Decision 2008/977/JHA shall be applicable.

Comment [U43]: Note that this authority is NOT the data protection authority. You can have two authorities involved, possibly more. The UK has followed this model and have a host of a "national supervisory authorities" each with with limited powers.

In the UK this provision fragments the system of regulation that protects the individual even further.

Comment [U44]: I would amend this to say that the national supervisory authority in relation to data protection matters has to be the national data protection supervisory authority, unless the national supervisory authority can offer a higher level of data protection regulation than the data protection authority.

I would also get the Member State to publish what the additional enhancements are.

CHAPTER IV: IMPLEMENTING MEASURES

Article 13: **Common protocols and supported data formats**

1. All transfers of PNR data by air carriers to the Passenger Information Units for the purposes of this Directive shall be made by electronic means or, in the event of technical failure, by any other appropriate means, for a period of one year following the adoption of the common protocols and supported data formats in accordance with Article 14.

2. Once the period of one year from the date of adoption of the common protocols and supported data formats has elapsed, all transfers of PNR data by air carriers to the Passenger Information Units for the purposes of this Directive shall be made electronically using secure methods in the form of accepted common protocols which shall be common to all transfers to ensure the security of the data during transfer, and in a supported data format to ensure their readability by all parties involved. All air carriers shall be required to select and identify to the Passenger Information Unit the common protocol and data format that they intend to use for their transfers.

3. The list of accepted common protocols and supported data formats shall be drawn up and, if need be, adjusted, by the Commission in accordance with the procedure referred to in Article 14(2).

4. As long as the accepted common protocols and supported data formats referred to in paragraphs 2 and 3 are not available, paragraph 1 shall remain applicable.

5. Each Member State shall ensure that the necessary technical measures are adopted to be able to use the common protocols and data formats within one year from the date the common protocols and supported data formats are adopted.

*Article 14:***Committee procedure**

1. The Commission shall be assisted by a committee ('the Committee'). That Committee shall be a committee within the meaning of Regulation […/2011/EU] of 16 February 2011.

2. Where reference is made to this paragraph, Article 4 of Regulation […/2011/EU] of 16 February 2011 shall apply.

CHAPTER V: FINAL PROVISIONS

Article 15: **Transposition**

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive at the latest two years after the entry into force of this Directive. They shall forthwith communicate to the Commission the text of those provisions and a correlation table between those provisions and this Directive.

When Member States adopt those provisions, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 16: **Transitional provisions**

Upon the date referred to in Article 15(1), i.e. two years after the entry into force of this Directive, Member States shall ensure that the PNR data of at least 30% of all flights referred to in Article 6(1) are collected. Until two years after the date referred to in Article 15, Member States shall ensure that the PNR data from at least 60% of all flights referred to in Article 6(1) are collected. Member States shall ensure that from four years after the date referred to in Article 15, the PNR data from all flights referred to in Article 6(1) are collected.

Article 17: **Review**

[Articles 17-19 are provisions are designed to avoid transparency and oversight. The suggested review mechanisms and statistical collections are not independent; they are fundamentally flawed and compromised by the conflict of interest that Member States/Commission have. To justify to the public the large amounts of money spent on this kind of surveillance there is a significant risk that self serving reviews and bogus stats will be produced. See also my EDPS comments on page 11]

On the basis of information provided by the Member States, the Commission shall:

(a) review the feasibility and necessity of including internal flights in the scope of this Directive, in the light of the experience gained by those Member States that collect PNR data with regard to internal flights. The Commission shall submit a report to the European Parliament and the Council within two years after the date mentioned in Article 15(1);

(b) undertake a review of the operation of this Directive and submit a report to the European Parliament and the Council within four years after the date mentioned in Article 15(1). Such review shall cover all the elements of this Directive, with special attention to the compliance with standard of protection of personal data, the length of the data retention period and the quality of the assessments. It shall also contain the statistical information gathered pursuant to Article 18.

Comment [U45]: THIS IS A POOR PROVISION AS ANY REVIEW IS NOT INDEPENDENT.

Comment [U46]: Remember that internal flights are to be included.

Comment [U47]: I would change this to get a Parliamentary Committee to do the Review or the Data Protection Authorities do the Review from a DP perspective.

What you can't have is Member States providing skewed evidence to a Commission that is likely to have a vested interest in the outcome of the review in favour of PNR data retention.

Comment [U48]: Even when the Article specifically relates to a review into data protection matters, this review might NOT be undertaken by the national data protection authority. The data protection authorities might not even be involved in the review at all. The risk of an unbalanced data protection review is therefore substantial.

Instead, the review is undertaken by the Commission which is proposing the interference in the first place. The Commission has a conflict of interest.

Any review thus risks being a self serving justification for the PNR Directive and of not much value as the Commission has its own self interest to protect.

I strongly suggest getting the EDPS or the WP29 or the EU Parliament doing this part of any Review.

Also this review will be based on the logs and information provided by Member States. THAT IS WHY THE CONTENTS OF LOGS SHOULD NOT BE AT THE WHIM OF MEMBER STATES. See comments at Article 11(4)

Comment [U49]: The data protection authorities should be able to insist on what statistics are collected from a data protection perspective. One can't allow the Member States or the Commission to provide whatever stats they consider relevant. The evidence base that justifies the Directive has to be independently sourced – otherwise it is compromised.

Article 18

Statistical data

1. Member States shall prepare a set of statistical information on PNR data provided to the Passenger Information Units. Such statistics shall as a minimum cover the number of identifications of any persons who may be involved in a terrorist offence or serious crime according to Article 4(2) and the number of subsequent law enforcement actions that were taken involving the use of PNR data per air carrier and destination.

2. These statistics shall not contain any personal data. They shall be transmitted to the Commission on a yearly basis.

Article 19

Relationship to other instruments

1. Member States may continue to apply bilateral or multilateral agreements or arrangements between themselves on exchange of information between competent authorities, in force when this Directive is adopted, in so far as such agreements or arrangements are compatible with this Directive.

2. This Directive is without prejudice to any obligations and commitments of the Union by virtue of bilateral and/or multilateral agreements with third countries.

Article 20

Entry into force

This Directive shall enter into force the twentieth day following that of its publication in the *Official Journal of the European Union.*

This Directive is addressed to the Member States in accordance with the Treaties. Done at Brussels,

ANNEX

Passenger Name Record data as far as collected by air carriers

(1) PNR record locator

(2) Date of reservation/issue of ticket

(3) Date(s) of intended travel

(4) Name(s)

(5) Address and contact information (telephone number, e-mail address)

Comment [U50]: This statistical analysis is NOT independent and risks Member States producing stats to justify the PNR Directive but not producing stats that point in the other Direction (e.g. there is nothing that allows a cost-benefit analysis to be done)

I would get the EDPS/WP 29 to identify what is statistics need to be collected. ANYBODY INDEPENDENT OF MEMBER STATES OR COMMISSION. THEY HAVE A VESTED INTEREST IN THE SUCCESS OF THIS DIRECTIVE AND JUSTIFYING THE MILLIONS SPENT ON THIS PROJECT.

The stats have to include costs, third country disclosures and a host of other things that won't be collected if Member States get their way.

The data protection authorities have to be able to define the content of logs and stats needed for a data protection analysis; the European Parliament could employ its own statisticians.

THIS PROVISION IS DESIGNED TO UNDERMINE WHAT LITTLE TRANSPARENCY THERE WILL BE

Comment [U51]: Member States can continue indefinitely existing agreements with each other outside the PNR Directive. This may allow really controversial exchanges to occur outside the minimal protection afforded by this Directive.

There is no provision to even list the PNR agreements outside the Directive. There is no attempt todraft the obvious: the Directive could easily have said that that such arrangements or agreements have to be brought into compliance with this Directive within **x** years (where x=3, 4 or 5).

Might be aimed at existing national security arrangements at a guess where Member States might not want to be "troubled" by data protection.. If this is the case, then national security should be made exempt from the provision.

Comment [U52]: Suppose it is incompatible with the Directive – what happens? Nothing as far as I can see.

You could have an amendment so that there has to be a bi-annual audit by the national data protection authority or supervisory authority to assess compatibility if the agreement continues outside the provisions of this Directive. Any audit report should be published unless exceptional circumstances apply.

(6) All forms of payment information, including billing address

(7) Complete travel itinerary for specific PNR

(8) Frequent flyer information

(9) Travel agency/travel agent

(10) Travel status of passenger, including confirmations, check-in status, no show or go show information

(11) Split/divided PNR information

(12) General remarks (including all available information on unaccompanied minors under 18 years, such as name and gender of the minor, age, language(s) spoken, name and contact details of guardian on departure and relationship to the minor, name and contact details of guardian on arrival and relationship to the minor, departure and arrival agent)

(13) Ticketing field information, including ticket number, date of ticket issuance and oneway tickets, Automated Ticket Fare Quote fields

(14) Seat number and other seat information

(15) Code share information

(16) All baggage information

(17) Number and other names of travellers on PNR

(18) Any Advance Passenger Information (API) data collected

(19) All historical changes to the PNR listed in numbers 1 to 18

Extract from Council Framework Decision 2008/977/JHA

Article 13

Transfer to competent authorities in third States or to international bodies

1. Member States shall provide that personal data transmitted or made available by the competent authority of another Member State may be transferred to third States or international bodies, only if:

(a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(b) the receiving authority in the third State or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;

(c) the Member State from which the data were obtained has given its consent to transfer in compliance with its national law; and

(d) the third State or international body concerned ensures an adequate level of protection for the intended data processing.

2. Transfer without prior consent in accordance with paragraph 1(c) shall be permitted only if transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third State or to essential interests of a Member State and the prior consent cannot be obtained in good time. The authority responsible for giving consent shall be informed without delay.

3. By way of derogation from paragraph 1(d), personal data may be transferred if:

(a) the national law of the Member State transferring the data so provides because of:

(i) legitimate specific interests of the data subject; or

(ii) legitimate prevailing interests, especially important public interests; or

(b) the third State or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law.

4. The adequacy of the level of protection referred to in paragraph 1(d) shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the State of origin and the State or international body of final destination of the data, the rules of law, both general and sectoral, in force in the third State or international body in question and the professional rules and security measures which apply.

Comment [U53]: There is no case-by-case limitation here so the provision could apply to mass data transfer.

Comment [U54]: There is no threshold test such as failure to disclose would prejudice a criminal investigation

Comment [U55]: Parts (c) and (d) are the provision that risks the politicisation of the decision making process with respect of transfer of PIU data to a Third Country.

For instance, Interior Ministers of a Member State might consent in return for some reciprocal favour or other or to repay some kind of favour.

Comment [U56]: See derogations from this provision at para 3 below

Comment [U57]: The use of the word "especially" means that the provision certainly applies to "important public interests" (e.g. terrorism) but also in other unspecified "interests" (e.g. which might not be of lesser importance).

The provision does not say that transfers can occur ONLY when there is an important public interest. It says that an important public interest is ONLY ONE of many unspecified criteria.

This provision allows Member States to make up the transfer rules to fit political objectives (i.e. transfers in the legitimate prevailing interests of the Government of the day).

Comment [U58]: This is another provision that can allow for wider transfer by "deeming" adequacy (e.g. as per existing exchanges between the Europe and the USA Authorities).