A COMMON EU APPROACH TO THE USE OF PASSENGER NAME RECORD (PNR) DATA FOR LAW ENFORECEMNT PURPOSES

IMPACT ASSESSMENT QUESTIONNAIRE TO DATA PROTECTION AUTHORITIES

Joint answer of the Article 29 Working Party

Introductory remarks

The Council requested the European Commission to develop a common EU approach to use PNR data for law enforcement purposes. In this context, the Commission requests input from Data Protection Authorities, Member States, and other stakeholders on the relevant positive and negative impacts, the necessary scope etc. of an EU approach to the use of PNR data. The Data Protection Authorities have decided to provide a joint answer to this questionnaire under the aegis of the Article 29 Working Party.

At this stage of the discussion, the Working Party cannot adequately address the request from the Commission. In order to adequately answer the questions posed and assess issues such as benefits and burdens (question 1), the necessary scope of a possible instrument (question 2), etc, the basic question to be answered is that of the necessity of the measures. An analysis of the necessity and purpose of the measures in light of the goals to be achieved, has to precede an impact assessment of the measures proposed.

In this context, the Article 29 Working Party has not seen any information presented by the Commission that would substantiate the pressing need to process PNR data for the purpose of preventing and fighting terrorism and related crimes, or law enforcement.

Evaluation of the necessity and proportionality of the measures can only be based on the experiences with the US PNR framework. A lack of available information in this context makes it problematic to assess the necessity, effectiveness and proportionality. Anecdotal information on the processing of API and PNR data by US authorities however concerns mainly passengers incorrectly identified as a risk to air security. The available information also indicates that primarily API data rather than PNR data are used in the context of the US passenger data framework.

For the reasons mentioned above, and until the Working Party is provided with clarification on these fundamental points, the Article 29 Working Party cannot conclude that the establishment of an EU PNR regime is necessary. Therefore, under these circumstances, the Working Party would be opposed to its development.

With regard to this position, the Working Party also takes into consideration that many other measures to make available personal data for the purposes of the fight against terrorism and organised crime, immigration control etc. have been or are being taken, the effect of some of which cannot yet be measured. Such measures include the Schengen Information System, the development of the Visa Information System, the obligation to provide API data under Directive 2004\82\EC, that is currently still being implemented in Member States, co-operation under the Europol agreement, the Prüm Treaty that will most probably be transposed into an EU instrument, etc.

The new measures under discussion in this questionnaire would entail the further processing of data collected by airlines for commercial purposes, for another public purpose of the fight against terrorism. To the extent that measures to be developed, be

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.
Office: LX 46 3/135. Telephone: direct line (32-2) 2955030 Fax: (32-2) 2967633.

they at EU level or at national level, entail a breach of Article 6 of Directive 95\46\EC and limitation to the right to private life, they should in any case respect the limits of Article 13 of Directive 95\46\EC and Article 8 of the European Convention on Human Rights.

The Commission will have to substantiate the pressing need for the processing of PNR data, in particular in light of the following:

- The operational need and purpose of collecting PNR data at the entrance of the European Union Territory.
- The added value of collecting PNR data in light of the already existing control measures at the entrance of the EU for security purposes, such as the Schengen system, the Visa Information System, and the API system.
- The relationship with Directive 2004/82/EC. Does the Commision already have information on the implementation of this directive and its effects?
- The added value of the processing of PNR data over the processing of API data.
- The use that is foreseen for PNR data. For identifying individuals in order to ensure air security? For identifying who comes into the territory of the EU? For general negative or positive profiling of passengers? Is there an interest in specific PNR fields for specific purposes of investigating and fighting particular crimes? Would PNR data be the most adequate data for these purposes?

Despite this position, the Article 29 Working Party has deemed it appropriate to fulfil the request from the European Commission and answer the questionnaire that has been sent to the Data Protection Authorities.

POLICY OPTION 1: DO NOTHING

The following benefits of Option 1 have been identified:

- No cost burden or other impact on national administrations
- No impact on EU relations with third countries

The following negative impacts of Option 1 have been identified:

- Fails to respond to European Council request for a common EU approach as would result in diverging policy from one Member State to another. Does not contribute to the objective of the Treaty on European Union (TEU) of creating an area of freedom, security and justice.

1.1 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations[1]), social (including fundamental rights[2]) or other impact of the option identified above.

[1] The costs for national administrations associated with different policy options are an important criterion for developing the policy. These costs might on the one hand include the investments needed to set up the necessary process/systems, and on the other hand the costs associated with running the system, i.e. the day-

Lack of harmonisation as such would not be sufficient ground for setting up an EU PNR system. Both national and EU level measures will have to fulfil the criteria of Article 13 of Directive 95\46\EC and Article 8 ECRM, as clarified above.

Provided the necessity and proportionality is adequately established and several Member States would be considering the development of a national PNR system, then harmonisation of such measures at EU level is to be preferred. The nature of international travel demands global solutions and so it would be strange not to adopt such a solution in this matter. Different approaches by different Member States leads to inconsistencies and uncertainty and differing rights for individuals depending on the local solutions adopted. A harmonised approach would also be beneficial for internal market reasons and will better serve the interests of the airlines.

The Working Party would have concerns about the unilateral approach as it is likely to lead to increased costs, for example, dealing with an increased number of complaints and concerns from individuals if different national laws with different standards were to apply. However, an EU level arrangement will not necessarily succeed in ensuring a sufficient level of harmonisation. It depends on the bandwidth of the measures. If Member States are allowed to implement national measures within a large bandwidth, the harmonising effect will be very limited, with all negative consequences described here above.

1.2 Can you identify additional impacts? If so, please assess them.

1.3. The negative impacts of Option 1 would outweigh any perceived benefit of this policy option, most notably since it fails to respond to the European Council request for common EU action in this field. Do you agree?

The Article 29 Working Party agrees with this statement for the reasons outlined above but wants to stress again that the question of negative impacts of Option 1 does only arise if the necessity of collecting PNR data in the EU for anti terrorism or law enforcement purposes has been proven as such.

POLICY OPTION 2: LEGAL INSTRUMENT

A legal instrument for a common EU approach to use of PNR data would take the form of a Framework Decision pursuant to Article 34 TEU. Within Policy Option 2, it is necessary to assess the impact of a number of alternative parameters:

Scope of instrument (forms of transport):

(1) Instrument limited to *airline* PNR data. **Positive impact** – covers scope requested by European Council; simpler and less costly to limit at least

---

to-day collection and dispatching of PNR data. The assessment of each of the options/parameters presented in this questionnaire should include the possible impacts on the costs for national administrations.

[2] Fundamental rights impact should cover questions such as whether a policy option promotes fundamental rights and notably protection of personal data, whether the policy may have the effect of targeting vulnerable groups or categories of people for example on the basis of ethnicity or religion and whether the various policy options have a differing impact on fundamental rights.

initially to *airline* PNR data. **Negative impact** – creates loophole that can be exploited by using other means of transport.

(2) Instrument covers passenger data limited to *air and sea*. **Positive impact** – Leaves fewer loopholes than (1). **Negative impact** – more complex than (1); more costly than (1).

(3) Instrument covers passenger data relevant to *air, sea and rail*. **Positive impact** – Addresses main forms of transport and so leaves fewer loopholes than (1) or (2). **Negative impact** – more complex and more costly than (1) or (2).

2.1 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

The broader the scope of the instrument is in terms of the form of transport, the broader the possible impact will be on the privacy of individuals and on the freedom of movement. It could possibly entail a near total surveillance of travel movements into and out of the EU. Broadening the scope implies stronger need for justification of the necessity, proportionality and subsidiarity of such measures.

What would be the purpose of collecting data from people travelling by boat or rail? Would it be to ensure boat or train security? If this is the case, what is the perceived threat from travelling by sea or rail? Would the purpose be identification of travellers into the EU? If that is the case, why would PNR data be necessary? The Working Party has not heard any case made yet for this information.

It is worth noting that the information given to sea and rail operators by passengers is normally less than the PNR data given to airline carriers. Boat and rail carriers, in addition, often do not collect passenger data, but rather sell tickets entitling the holder to use the service.

The Working Party does not consider justified any solutions whereby private companies such as carriers are caused to request even more information from sea and rail passengers - information that they do not need to run their services – for public purposes. This would also increase the surveillance of all travel movements into and out of the EU, with strong effects on privacy and the freedom of movement.

2.2 Can you identify additional impacts? If so, please assess them.

2.3 The benefits of limiting the instrument's scope to use of *airline* PNR data would outweigh the benefits of a broader approach covering other forms of transport. Do you agree?

In principle the Working Party agrees, in the context of the comments made above and the need to proof that even the collection of airline PNR data is proportionate.

Scope of instrument (geographic):

(1) PNR data for international flights[3] originating in a third country to the territory of at least one Member State of the European Union. **Positive impacts** - includes PNR data most likely to be relevant to address threat within EU territory. **Negative impacts** – Does not facilitate situation where third country requires reciprocity of PNR data.

(2) As for (1) and including also PNR data for international flights from the territory of at least one Member State of the European Union with a destination in a third country. **Positive impacts** – covers PNR data most likely to be relevant for threat assessment in EU territory and addresses availability of outgoing data which may be needed on a case by case basis if third country requires reciprocity. **Negative impacts** – may be more complex and costly than (1).

(3) As for (2) and including also PNR data for internal EU flights originating in one MS and terminating in another MS. **Positive Impacts** – covers widest scope of flights. **Negative impact** – including internal EU flights may be disproportionate, as may not present significant added value by comparison to its complexity; could appear to be in contradiction from the legal and political points of view, with free movement of people within the EU

2.4 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

A similar argument as provided under 2.1 can be made here with regard to the impact on human rights of an extension of the scope of the instrument. A near total surveillance of all travel movements into and out of the EU could be the consequence, with strong effects on privacy and the freedom of movement.

The geographic extent of the measures must be founded on a clear understanding of the pressing need that the legislation is meant to address, taking duly into account the effects on human rights mentioned here above.

With regard to option 2: The possibility of future requests for PNR from third countries does not provide sufficient justification. Therefore, the Working Party would oppose this option. Reciprocity will only be acceptable under very strict conditions and in respect of third countries that guarantee an adequate level of protection.

With regard to option 3: The Working Party agrees that this option could be in contradiction with the free movement of people within the EU. This is particularly the case if the data are used for immigration related purposes. Therefore, the Working Party does not favour this option.

However, if the sole purpose would be the prevention of terrorism and directly related aviation security, a differentiation between flights within the EU, including internal flights within one Member State, and other flights is in itself not logical. This would have to be substantiated on the basis of a risk assessment for various flights. In any event, it has to be examined whether the collection of data about

---

[3] Subject to the answer to 2.2, the reference to international flights may also be read as including passage by sea and / or rail.

internal EU flights is necessary in view of the other (already existing) legislative measures, that provide relevant information.

In addition, it is unclear how broad any of the proposed options above would be. Will the legislation to be developed define the (third) countries from which PNR data will have to be collected? And at what level will these options be decided? At community level, or will it be left to Member States to fill in the specific countries (as is now the case with Directive 2004/82/EC)? If the latter option were to be chosen, what is the view of the Commission on the level of harmonisation reached?

2.5 Can you identify additional impacts? If so, please assess them.

2.6 The benefits of limiting the instrument's scope to PNR data for international flights to and from the EU would outweigh the benefits of a narrower approach limited only to incoming EU flights. Do you agree?

The Working Party does not as such agree with that. It again depends on an evaluation of the necessity of collecting data from flights leaving the EU. For what purposes are the data to be used?

2.7 The negative impact of including all EU internal flights would outweigh its potential benefit. Do you agree?

Yes

Use/Purpose of collecting PNR data:

(1) Preventing and fighting terrorism and related crimes. **Positive impact** – focuses on core area identified by European Council. **Negative impact** – narrow and misses potential for PNR data to play broader role in fight against organised crime.

(2) Preventing and fighting terrorism and related crimes and other serious crimes, including organised crime, that are transnational in nature. **Positive impact** – broader scope to maximise the potential value of PNR data; broadly in line with PNR Agreements with third countries.

(3) Preventing and fighting terrorism and related crimes and other serious crimes, including organised crime, that are transnational in nature as well as for more general public policy purposes, including fiscal and social security checks. **Positive impact** – broad scope to maximise value of data but **Negative impact** – likely to cause significant concern about data privacy and proportionality.

2.8 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

The Article 29 Working Party emphasises that the use of PNR data for the more general purposes described under (3) would certainly be disproportionate. It would create the possibility of unjustified surveillance of people on a very large scale by the public authorities.

As stated in the introductory remarks, the necessity to collect PNR data for the purposes stated under (1) and (2), has not yet been substantiated. In particular, the Commission will have to clarify why current measures to fight "other serious crimes that are transnational in nature" would not suffice. What would be the added value of PNR data?

In addition, the categories of "related crimes" and "other serious crime" that is "transnational in nature" are too vague and would need a much more precise description taking into account the jurisprudence of the European Court of Human Rights. Also, the necessity of the various categories of PNR data would have to be explained.

In this context, the Working Party would like to reiterate that clarification is needed about the intended use of the PNR data, i.e. for identification purposes, profiling, or other usages.

2.9 Can you identify additional impacts? If so, please assess them.

2.10 The positive impact of limiting the instrument's scope to preventing and fighting terrorism and transnational organised crime would outweigh the benefits of a narrower approach limited to counter terrorism. Do you agree?

Not necessarily, as clarified in the answer to question 2.8.

2.11 The negative impact of allowing data to be used for broader fiscal / social security purposes outweigh the benefits. Do you agree?

We agree with this statement for the reasons stated above.

Data retention period:

(1) Data to be deleted on arrival of passenger in destination country. **Positive impact** – reduces risk of data abuse and may enhance data protection. **Negative impact** – may only be realised at later stage that data relate to identified suspect; Significant difference between EU retention period and retention period for EU PNR data of some third countries.

(2) Data to be deleted after a period of three and a half years from the date of transfer to the Passenger Information Unit (or other designated body). **Positive impact** – Allows scope for access to and use of data where suspicion identified at appropriate stage after flight;

(3) retention period in line with EU/US and EU/Canada PNR agreement. **Negative impact** - Period may be regarded as disproportionately long.

(4) Data to be deleted after a period longer than 3.5 years from the date of transfer to the Passenger Information Unit (or other designated body). **Positive impact** – allows flexibility but **negative impact** – would be seen as excessive and not respecting data protection concerns.

2.12 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

Data must be retained for the period of time that is necessary for the purposes for which the data are collected. If, for example, identification of travellers posing a threat is the purpose, there would not be sufficient ground for retaining the data for longer than the retention period established under Directive 2004/82/EC. That directive states that data should be deleted 24 hours after arrival.

The retention of personal data of unsuspected individuals for possible future use for the given purposes has a substantial impact on human rights and would therefore need strong justification.

It is our understanding that the period of 3.5 years was decided on during the drafting of the EU-US international agreement and supporting undertakings, as that was the lifespan of that agreement. This does not provide sufficient ground for an EU retention period of 3.5 years.

2.14 Can you identify the most appropriate data retention period bearing in mind data protection concerns on the one hand and potential law enforcement benefits on the other?

A substantiated fixed retention period should be based on the purposes of the processing. The Working Party would support a short and proportionate period of time.

2.15 A medium term retention period of 3.5 years outweighs the benefits of deletion on arrival (too short) and deletion after significantly longer period. Do you agree?

We do not agree with this statement. Any retention period needs to be founded on the clearly justified needs of the processing of the data, be proportionate and be consistent with other retention period decisions in similar fields.

Exceptions to data retention period:

(1) No exception to strict data retention period. **Positive impact** - reduces risk of data abuse and may enhance data protection. **Negative impact** - inflexible.

(2) Retention period to be extended where specified PNR data are used for "crime investigation" or for "crime intelligence operation" as defined in the draft Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States. In this case data to be retained during course of intelligence operation, investigation and, as appropriate, prosecution. If person is convicted, data can be retained as necessary. If no conviction, data are destroyed. **Positive impact** – Flexible approach taking account of law enforcement needs and data protection concerns.

2.16 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

It is unclear what kind of processing is foreseen in the description under (2) above. It seems to foresee some form of standardised linking with databases on crime investigations and crime intelligence operations, which is outside the proposed purposes of the processing of PNR data. This would not be acceptable.

In case there is a hit with the system, it should obviously be possible to retain personal data for longer. Any other exceptions to the general retention period

should be very restrictive and related to the purposes for which the PNR data are processed. Case-by-case exceptions to the general rule are possible on the basis of other relevant legislation.

2.17 Can you identify additional impacts? If so, please assess them.

2.18 Can you identify other possible exceptions to the usual data retention period?

If there have been abuses of the system and data is needed to assist with an audit trail or any investigation. If an individual is arguing over the accuracy of the data about them, the data must be preserved to allow individuals to exercise their rights under the Directive and national law.

2.19 The law enforcement benefits of a flexible approach which allows retention of PNR data in appropriately justified cases, outweighs the benefits of an approach which focuses only on data protection. Do you agree?

We do not think this question is accurately worded. It needs to contrast the flexible approach allowing retention in appropriately justified cases with the approach focusing on fixed retention periods - not data protection. Data protection law states that data should not be kept for longer than is necessary for the purpose it was collected for. In addition further processing for other purposes, which could also entail longer retention periods, can be justified as well in case this processing is compatible with the initial purpose. The focus is on the continued need for a (compatible) purpose, so it does not conflict with data protection law.

Body receiving PNR data:

(1) Member States to set up or designate a "Passenger Information Unit" responsible for receiving, requesting, analysing and disseminating to the competent national authorities the Passenger Name Record data provided by air carriers[4]. **Positive impact** – Would facilitate efficient transmission of PNR data from air carriers to relevant national entity; existence of single dedicated entity at national level may facilitate requests for and onward transmission of PNR data between Member States. **Negative impact** – implies deployment of human and financial resources and so involves cost.

(2) Receipt of PNR data to be centralised within EU and possibly operated by a centralised system. **Positive impact** - efficiency of a "single window" receiving and giving access to European PNR. **Negative impact** – vast amount of data and carriers mean that centralised systems would be complicated, possibly unworkable and may raise data protection concerns.

2.20 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

The Working Party would agree with a distributed approach that keeps the data as close as possible to its source. There needs to be appropriate and consistent safeguards that can be enforced. Unless strict use limitations are set and

[4] Subject to the answer to 2.2, the reference to air carriers may also be read as including passage by sea and / or rail.

safeguards developed, such as effective access prevention by using up to date cryptography, the risks of a centralised database are many and varied, particularly as regards security, where access could be granted to an extensive collection of data.

2.21 Can you identify additional impacts? If so, please assess them.

2.22 The benefits of establishing or designating a dedicated national Passenger Information Unit would appear to outweigh attempts to put in place a centralised EU system. Do you agree?

The Working Party agrees with this statement for the reasons outlined above.

Method of transmitting PNR data to PIU or other relevant body:

(1) Push Method. **Positive impact** – Preferred option from data protection point of view; removes risk of interference with data by relevant public body. **Negative impact** – technology not yet fully developed by airlines; cost to airlines.

(2) Pull Method. **Positive impact** – technology exists now. **Negative impact** - risk of damage to airline data; less preferred from data protection point of view; cost to airlines.

(3) Hybrid – airline transfers data to secure mail box to which only the PIU has access. **Positive impact and negative impact** are likely to be the same as for (1).

2.23 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

The Working Party is in favour of the push principle. The advantage of a push system is that the control over the sending of the data remains with the data controller. Only necessary and relevant data is transmitted rather than allowing access to a carrier's system with all the risks that entails. It is unclear how the hybrid system will work in practice. If it pushes all the data to the secure mailbox, then how is this different to the pull system? It would still rely on trusting the receiving authority to only take the data they need. If a hybrid system would however have built in technical measures ensuring controlled access by public authorities to the data, such a system could also have benefits: It would perhaps diminish costs for airlines, high security levels could be set, and it would provide a better opportunity for supervision and oversight, which could also contribute to increased transparency. In addition to that, the use of Privacy Enhancing Technologies could ensure that authorities would only get access to those personal data that match their lists of risk passengers.

2.24 Can you identify additional impacts? If so, please assess them.

2.25 The push or hybrid systems would appear to have equal benefits over a pull system. Do you agree?

Both systems are to be preferred over a pull system. The push principle is crucial: control over the provision of data should remain with the airlines. In addition,

supervision should be possible. However the drawbacks and positive impacts of a hybrid system would necessitate further study.

Bulk or case by case transfers:

(1) The PIU or other relevant body receives bulk PNR data and transfers bulk PNR data to other competent authorities. **Positive impact** – relative simplicity. **Negative impact** – raises data protection concerns.

(2) The PIU or other relevant body receives bulk PNR data which are automatically filtered within the PIU to screen out data of non-suspect persons. PIU then transfers data on a case by case basis to other competent authorities. Benefits – addresses data protection concerns by minimising transfer of data of non-suspect persons. **Negative impact** – law enforcement may consider more useful to trawl against broader data sets.

2.26 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

The two options above focus on bulk or case-by-case transfers. It is important to note that both scenarios start from the presumption that the PIU or other relevant body is receiving bulk data. The important point for data protection here is that the PIU or other body only gets the relevant information from the carrier, as well as only transferring relevant information. (Technical) solutions should therefore be sought which allow only for the provision of relevant information to the PIU or other receiving body .

Bulk transfer of personal data, which would include data of unsuspected travellers, to other authorities would be disproportionate, as data may only be provided to an authority if necessary for a given purpose. This would automatically entail case-by-case provision only.

2.27 Can you identify additional impacts? If so, please assess them.

2.28 The data protection benefits of ensuring appropriate screening within the PIU and that data are transferred from the PIU to other competent authorities on a case by case basis, would appear to outweigh any likely benefits of the PIU transferring bulk data. Do you agree?

We agree with the statement but reiterate that this option is still not preferable to that of making sure that only the necessary data is sent in the first place.

Onward Transfer of PNR data by PIU or other relevant body:

(1) Onward transfer only permitted to national competent authorities responsible for combating terrorism and other serious crime. **Positive impact** - simple but **negative impact** – does not facilitate other Member States' use of that data for own investigation purposes.

(2) As for (1) but onward transfer also permitted to other Member State competent authorities responsible for combating terrorism and other serious crime. **Positive impact** – Facilitates use of PNR data for Member States' investigation purposes. **Negative impact** – Receiving MS "loses control" of data though data remain within EU.

(3) As for (2) but onward transfer also permitted to third country competent authorities responsible for combating terrorism and other serious crime. **Positive impact** – Promotes broader use of PNR data. **Negative impact** - Receiving MS "loses control" of data and data leave EU.

2.29 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

In principle, onward transfer of the data to another Member State should be possible on a case-by-case basis for the purposes of this legislation. Thus, this should not include a priori "other serious crime". In addition, the concept of "competent authority" (and "other serious crime") would have to be clarified. The authorities should be competent for the purposes of this legislation. There should be sufficient data protection safeguards. In this context, the Working Party reiterates the importance of the adoption of the Framework Decision for Data Protection in the third pillar, which would ensure a high and equal level of third pillar data protection throughout the EU.

In case of transfers to third countries, the third country should ensure an adequate level of protection.

2.30 Can you identify additional impacts? If so, please assess them.

2.31 Facilitating onward transfer at national level and within the EU would be beneficial with case by case transfers of data to third countries also being possible. Do you agree?

See the answer given above.

Security of Data:

(1) Specify appropriate common encryption levels. **Positive impact** – provides certainty about data security. **Negative impact** – may be disproportionate to require common approach on encryption; likely cost issues in particular to air carriers.

(2) Require common transmission protocols. **Positive impact** – may significantly reduce air carrier cost and may enhance onward transfer. **Negative impact** – may be difficult to agree common protocol and could raise competition issues.

2.32 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the options identified above.

Firstly, any level of security needs to be appropriate to the sensitivity of the data involved and the harm a breach of security may cause. Higher harm potential of data, calls for higher security. These two options focus purely on transmission mechanisms, whereas security is wider than this. These options fail to recognise the potential for breaches of security that take place outside the transmission process.

2.33 Can you identify additional impacts? If so, please assess them.

2.34 The benefits of common transmission protocols would outweigh the potential downside. On the other hand the potential benefits of insisting on common encryption standards would not appear so great as to justify this requirement. Do you agree?

This question is not clear to the Article 29 Working Party. Any technical solution will have to ensure a high level of protection proportionate to the risk posed. Common transmission protocols cannot be said to be better than encryption standards. Both are needed, and what is important is that both are appropriate to the sensitivity of the data and the harm that a breach of security may cause. In addition, security of data relates to technical, human and organisational aspects, and not only to transmission of data.

A common approach throughout the EU is most probably preferable, as it is likely that the reduction of costs for air carriers outweighs the resources that are engaged in reaching this kind of agreement.

POLICY OPTION 3 - ENCOURAGE COOPERATION BETWEEN MEMBER STATES

The following negative impacts of Option 3 have been identified:

- If the problem i.e. terrorism and other serious crime, is limited to a small number of countries, a policy option designed to encourage cooperation among this small group may be the appropriate solution. However, these problems, particularly organised crime cannot be said to be limited to a small group of Member States. Accordingly, cooperation would not appear to present the optimal solution.

- Difficult to ensure a common EU approach if by means of encouraging cooperation only.

3.1 Please assess the relevant positive and negative impacts, namely economic (including costs for national administrations), social (including fundamental rights) or other impact of the option identified above.

The emphasis under this option seems to lie on co-operation in the fight against "other serious crime" and "organised crime". If that is the case, it is unclear why current co-operation mechanisms, such as Europol, would no longer be considered sufficient.

If however the necessity of the proposed measures is substantiated and Member States wish to develop a PNR policy, option three is not to be preferred. Option three will lead to different amounts of information being provided by and to Member States, which leads to inconsistency, uncertainty and a lack of protection for individuals. There would be different standards due to some Member States acting as part of co-operation arrangements and others acting under legal compulsions. There would be inconsistencies with issues such as further use and retention. This option would give less legal certainty over co-operation arrangements and could lead to more uncertainty about obligations and rights for organisations and the public. There would also be less transparency over co-operation arrangements.

3.2 Can you identify additional impacts? If so, please assess them.

3.3 The **negative impact** of Option 3 would outweigh any perceived benefit of this policy option, most notably since it fails to respond to the European Council request for a common EU action in this field. Do you agree?

The Working Party agrees, under the conditions given in the answer to questions 3.1 and 1.1 above. A failure to respond to a European Council request for common EU action is in itself however not sufficient justification for EU measures.