Annex

1. GENERAL APPROACH

- The new approach of the Checkpoint of the Future is "to move away from the rigid and predictable “one-size-fits-all” approach that characterizes today’s passenger security screening environment to a risk based approach based on security outcomes, process improvement, and technology." (p. 3)

- This approach raises fundamental questions about how compliance can be ensured with the data protection principles as enshrined in the EU data protection legal framework (Directive 95/46/EC and Council of Europe Convention 108 -as well as the Recommendation on profiling), in particular on:
    - the principles of necessity and proportionality;
    - data quality, data minimisation and purpose limitation;
    - special categories of data;
    - legitimacy of the processing;
    - data subjects' rights and transparency;
    - automated decisions and profiling;
    - international transfers of personal data,
    - data security and confidentiality.
- Privacy by design should be a guiding principle. We have heard from some stakeholders that the project has first to be developed and tested before privacy issues are taken into account. Privacy concerns should on the contrary be taken into account from the very first stage of the conception of the project. Otherwise, it might be difficult to take personal data protection on board at a later stage.

2. EFFECTIVENESS

- Before deciding on its implementation it should be demonstrated that the project is really effective. Note that in the case of body/security scanners, despite some pilot tests, only after their implementation in several countries it was realised that they were not effective enough.

- One of the arguments for such a project is making airport security checks more cost-efficient. This could be contradictory, as implementing something similar to the IATA checkpoint of the future would require important economic inversions. In addition, some of the proposals seem to render the check lengthier, as there will be more controls and, in any case, random controls will not completely disappear.

3. NECESSITY AND PROPORTIONALITY

- Is there really a need for such a project? Is there a real demand from citizens / passengers and from most governments?

- What evidence is there to suggest that passengers would be happy with such data collection or believe it would be beneficial?

- What evidence is there to suggest that this a necessary and proportionate response to this issue?

- Will the potential improvement to be brought by the project be so important in terms of security, passenger experience and costs to compensate the major intrusion to privacy that it will cause?

- Are there any alternatives to this process?

4. PASSENGER DIFFERENTIATION

- What does "passenger differentiation" mean and how can it be implemented in compliance with the principles of data protection?

- How does passenger differentiation relate to the provisions of European law on automated individual decisions?

- Do the rules of the Schengen Border Code exclude or limit passenger differentiation?

- Who is making the assessment necessary to distinguish between the risks passengers seem to present? What are the limits for the co-operation between airlines and government?

- Is it possible to make a reliable statement on the risk of a passenger? What criteria is the risk assessment based on? What research and scientific proof underpins the method and the value of the risk assessment? What kind of information and what amount of information would be necessary?

- The document *Checkpoint of the Future - Executive Summary* mentions "Rules based analysis of reservations and check in data" (p. 10-11). In particular, does this mean that past reservations/travels will be a factor in the risk assessments (for example for the known travellers, will past flights be recorded and stored in a database somewhere that would be accessed to include in the risk assessment for subsequent flights for these known travellers)?

- What are the limits to take particularly sensitive factors into account, such as race, gender etc?

- Is it planned that the information collected will be stored after the assessment?

- What information would be transferred to whom?

- What experiences do exist with "scoring" in the other areas?

5. DATA, DATA CONTROLLERSHIP AND COMPLIANCE

- Which data will be used within the framework of the Checkpoint of the Future? What is the source of these data and what would be the required legal basis for the processing of such data?

- How long and by whom will the data be retained? Plus, what laws, codes of practice etc will this be based on?

- Who will ensure the reliability/integrity of data when it is matched?

- Who is liable for inaccurate/unlawfully stored information?

6. PURPOSE LIMITATION

- What safeguards will be in place to ensure that this data is used only for the specific purpose it is collected for? For example not using it for marketing.

- Which will be the purpose of the processing operations foreseen in the project? The reply to the question of proportionality might be different depending on whether the purpose is the fight against terrorism, the fight against serious crime, or the fight against any crime or offence.

7. KNOWN TRAVELLER PROGRAMMES

- Will the national traveller program become compulsory?

- What will be the legal basis for this? Is it consent? If so is it arguable that this is not freely given as defined in Section 2(h) of Directive 95/46/EC?

- Will there be mutual recognition of all RTPs?

8. BEHAVIOUR ANALYSIS

- To what extent can the use of behaviour analysis be based on research and scientific evidence?

- How reliable are the algorithms for behavioural analysis?

- In case it is done automatically, need to respect Art.15 current Directive (future Article 20).

- Will the results of behaviour analysis on passengers be stored and/or communicated between stakeholders?

9. SUBJECT ACCESS AND TRANSPARENCY

- Who will be responsible for fair processing and subject access requests?

- Will the passenger be informed, how?

10. IDENTITY MANAGEMENT

- Is any work planned to ensure a minimum level of security assurance for passport delivery (i.e. ensure that all countries deliver passport that are trustworthy)?

11. ACCESS TO DATA AND DATA SHARING

- To which authorities or organisations will the related personal data be transferred in order to analyse them and take decisions based on them?

12. TECHNOLOGY

- What does "remote image processing" mean? How would it be implemented?
- What systems are used for biometric verification at eGates?
- What kind of security scanners (body scanners) will be used?
- Who will transfer what information to whom? Will it be encrypted?

<u>For all Blueprints</u>

- Secure passenger information network: Could you please elaborate on the network that is foreseen to be implemented to cover all the requirements of these blueprints? What is the scope of the network? What are the endpoints? What are the services provided on the network? Who manages the network? Who can access the network? How is information on the network protected and logged?
- Would the shared data between states be stored somewhere? Who will be responsible for it? How will it be protected?

<u>Blueprint 2017</u>

- It is mentioned that there will be "limited connectivity to checkpoint". Could you please elaborate on what the endpoints are in this case? What covert and overt behaviour analysis techniques will be used and how will they work?

<u>Blueprint 2020</u>

- What is meant by "stand-off" identity management system?