

**Report on Article 29 Working Party Workshop on an EU approach towards a new
passenger data agreement
Monday, 26 March 2007, Brussels**

The Article 29 Data Protection Working Party, stressing its constructive role in the ongoing discussions on a future PNR Agreement with the US, organised a workshop in Brussels with experts in the field of passenger data to examine the privacy issues of the current interim agreement and a future deal. Negotiations on a new long-term agreement covering the flow of data of millions of passengers annually have already started. Participants of the workshop included representatives from the European Commission, national governments, the airline industry, researchers and members of the European Parliament and of national parliaments. The sessions were chaired by Mr. Stavros Lambrinidis, Vice chairman of the European Parliament's LIBE committee. Mr. Peter Schaar, Chairman of the Article 29 Data Protection Working Party, presented a welcome address and some conclusions of the workshop.

The workshop consisted of three panel sessions dealing with various legal and technical aspects of the transfer of passenger data to the US Department of Homeland Security (DHS). The aim was to come to a common approach which strikes the right balance between security demands, fundamental rights and economic concerns. The main results of each panel shall be briefly summarised below.

Panel 1: State of play and factual information on passenger data issues

Mr. Faull, Director General at the European **Commission** began by giving a brief outlook regarding the current negotiations with the US. It was stressed that the key issues would be the same as during the previous negotiations, namely what data is to be collected and processed; for how long will it be stored; the issue of onward transmission; as well as the technical aspects. The Commission mentioned that the US have no objection to using the push system, that some airlines are already pushing data and that others are ready to do so. The issue of reciprocity is not a feature of the negotiations, as there is currently no PNR system across the Union. The Commission is considering such a plan; however, this would perhaps not be supported by all member states.

Mr. Camus, representing the **Association of European Airlines**, emphasised that the airlines are also seeking legal certainty and clarity. Specifically, they would like to see a stable framework and different authorities having a consistent approach. They would also like to find a cost efficient solution and the representative pointed out that each change to an existing system requires additional investments. A solution which involved a limited number of transactions, possibly with a single transmission point ("single window" principle) for data requested from the EU could be a feasible option. Regarding the transition to push, AEA mentioned divergences in interpretation of the present framework: the problem seems to lie in terms of additional pushes, i.e. automated requests for a push, over which the airlines have no control. Finally, AEA expressed the wish of airlines to be more involved in the process, in order to be able to inform the parties involved of what is possible and what is not. The issue of compensation for airlines was also raised, as airlines perform tasks of law enforcement agencies. He also mentioned that in case of a PNR system across the Union, the EU should learn from the experience with the API directive.

Mr. Smith, from the **UK DPA**, outlined some concerns regarding the transfer of PNR data in terms of protecting the rights of the individual. Essentially, he would like to see

the same level of protection for data transfer as in the European data protection system, under Directive 95/46/EC. The lack of data protection framework for the third pillar complicates the issue, but nevertheless, an adequate level of data protection must be provided. This can only be achieved through an EU solution, not through bilateral ones. Specific concerns regarding PNR include: the amount of data collected (are 34 fields really needed?), the practical use of the data (how valuable is the analysis?), retention periods (more than 3.5 years is disproportionate), transparency (as WP 29 has emphasised in the past, passengers should before they travel be provided with information regarding how their data will be used, so that they can make a decision whether or not they want to travel), the right of redress and the issue of purpose limitation (a line must be drawn for onward transfers and attempts to use the data for other purposes must be resisted). Furthermore, it was mentioned that certain aspects of the agreement which are positive in terms of data protection should be preserved, such as the non-transfer and non-use of sensitive data and the collection and use of additional information which is not usually collected by airlines (such as home address and mobile number). Finally, the need for trust and confidence was emphasised. Supervision in the form of the Joint Review would be a useful tool to maintain trust that the Undertakings are being honoured. In addition, the Undertakings should become a legal obligation; there is concern that this is not the case and they have already been altered by the US.

In the following discussion, the question was raised where the responsibility begins and ends for private enterprises and what possibilities there were for putting the discussions in the public domain and so ensuring more transparency.

Mr. Hosein from Privacy International expressed concern that the EU appears to be satisfied with the current terms of the agreement, which in fact contains provisions which would have been unacceptable four years ago (e.g. 3.5 year retention period was considered too long; use of data beyond counter-terrorism was not acceptable; wanted a periodic review and this has only taken place once etc). In this context he asked if the goal posts had been moved since initial negotiations.

On the issue of transparency, Mr. Faull stated that negotiations have to remain confidential, as it is a matter between governmental authorities. Private enterprises can therefore not be present at the negotiating table. As to the issue of the goal posts having been moved, he said that this was a matter of judgement and that the initial starting point was different. He also emphasised that the US wants an agreement. Theoretically it can manage without one and take unilateral action, but it has not done so for commercial and political reasons.

Panel 2: The technical solutions

Ms. von Reden from **IBM** gave a presentation on technology which allows data to be exchanged in an anonymised way. This technology has actually existed since 2001 and has been used between intelligence agencies. A "one way hash" converts messages into algorithms, which are then stored in a "resolver" (which is neither a government authority nor an airline, but a "trusted third party"). Only if there is a match detected between 2 numbers (i.e. a number on a watch list and a number on a list of passengers) is an alert sent to the government, who then asks the airline to lift the anonymous status. In addition, there are management tools which handle complications such as passengers with the same name, date of birth, different ways of writing date of birth etc.

Mr. Simmons from **Amadeus** gave a presentation on the implementation of the push system. This software was finalised in October 2005. The system was implemented with Canada in April 2006 and implementation is due to take place with UK customs in April 2007. Implementation with the US is described as being "stop-start" with 14 activities

still remaining to be implemented (for example, to establish support processes, as well as process and software access issues related to the ad hoc push). He offered no timeframe for the conclusion of these outstanding issues.

Mr. Grande from **Lufthansa** put forward AEA's proposal for the collection and the transfer of passenger data via the ADEL concept in a privacy enhancing way. He stressed that even if the respective emphasis is different, all parties involved (government, passengers and airlines) actually have the same goals. He also suggested that governments and passengers make more use of existing channels and databases, rather than completely relying on airlines to achieve the solutions. Although airlines can support this process to a certain extent, a major part of the required information is already available in government databases.

Ms. Kotschy from the **Austrian DPA** presented the "Austrian solution", which was developed as a result of the EC being formally invited to come up with ideas for technical solutions for transferring PNR data to the US in 2003. This system consisted of a single transfer point for PNR data ("PNR Gateway"), open to all airlines as an access point for the US CBP. The system was not implemented as there was a problem with financing. This was because at the time it was unclear if providing the solution was the task of airlines or the Member States and the EU. This issue has since been clarified by the ECJ. The system acknowledges the third pillar aspect of PNR, takes on public responsibility and it also spreads the financial burden of PNR transfer to all stakeholders. In addition, such a system with a single transfer point will become necessary if the EU member states adopt the idea of PNR data transfers for flights into the EU.

In the following discussion, questions were raised about the privacy enhancing technologies that had been presented. Although the technology enables data to be made anonymous, this anonymity only remains in place until there is a match. Once anonymity is lifted, there is no control on how the data is used or further processed. With regard to the push method, the necessity to keep an open mind was mentioned. It would be dangerous to regard one commercial product (i.e. Amadeus) as the only solution.

Panel 3: purpose and necessity for using API and PNR data

Mr Rymer from the **UK's e-borders programme** gave a presentation on Project Semaphore, which is a multi-agency "border management" programme in place since November 2004, which uses API and PNR data. The purposes are not limited to counter-terrorism, but also cover areas such as illegal immigration and pursuing "serious crimes" (murder, rape, drug trafficking). The aim is to improve border security by a proportionate use of data to target specific risks effectively, without inconveniencing genuine travellers. The fact that PNR is available up to 48 hours prior to departure means that authorities can intervene before travel commences. For example, receiving PNR data early led to the intervention before boarding at one point of embarkation of 18 people and the arrest of a suspected facilitator. The use of PNR records has also proven effective in tackling drug trafficking and asylum abuse. The error rate is also said to be very low.

Mr. Gozi, an **MP from the Italian Parliament** stressed the need for national parliaments to be more involved, so that there is a parliamentary and public debate to give governments guidelines before they act in Council. He also pointed out that parliaments often are not given timely and proper information. The situation is rendered even more difficult due to the legal "grey area" between the first and third pillars - this increases the need for public scrutiny. For example, the interim agreement was not submitted to parliamentary ratification in all states and even in those states where it was, the agreement entered into force, prior to ratification. He suggested making more use of

the existing international agreements and structures, such as the ICAO and developing a global approach. In addition, new synergies should be developed between national parliaments and the European Parliament. The current agreement should be assessed as well as the impact of the API directive. Security cooperation should be put into a wider context and citizens should be given the certainty that their data is collected for their protection and not for other purposes.

Ms. In't Veld, MEP and rapporteur on PNR, pointed out that the problems associated with PNR processing and transfer stem from their questionable effectiveness and justification. Evidence on the value of PNR analysis is highly restricted as this is deemed to be a matter of national security. However, the original purpose of combating and preventing terrorist attacks has since been considerably expanded. She emphasised that lawmakers require more facts and figures and that due to the present lack of transparency, there is no democratic control. She specifically demanded information regarding: false positives, how many attacks have been prevented and reasons for the massive growth of people on watch lists. She also examined the question of whether there was evidence that PNR processing was in fact not useful. There are indications that the US can actually manage with fewer fields of data, as an average PNR rarely contains more than ten elements. Furthermore, the accuracy of the data is highly questionable; approximately half the data in records may not be accurate. The proportionality of the measures was called into question - is this the only way to achieve the objectives? Is there perhaps a less intrusive way? She pointed out that the data is being mainly used for profiling and that this in effect eliminates the presumption of innocence. Finally, she states that the European Parliament wants the effectiveness of the present agreement to be assessed before a new one is concluded.

The following discussion focused mainly on Mr. Rymer's presentation, for instance on the legal basis for e-borders, as well as issues such as retention periods and error rates. Mr. Rymer said that secondary legislation is planned for e-borders and UK position has not changed as regards border security and Schengen. He also said that there is a very low error rate; for example in 8000 alerts, only a very small number turned to be the wrong person. Mr. Smith mentioned that the UK DPA had been involved in the early stages of e-borders and in the Project Semaphore. There had been concerns regarding transparency and information to passengers, which have been dealt with. However, there are still unresolved questions about retention periods. What has also changed since the early stages is the expansion of the legal basis to collect more information than was originally possible.

Conclusions

- **The new agreement should respect fundamental rights**, and more specifically Article 8 ECHR, Article 8 of the EU Charter of Fundamental Rights and the provisions of the CoE's 108 Convention. This could best be achieved within an appropriate legal framework in place in the form of an FD on data protection in the third pillar.
- There is a need for **clear and precise minimum standards at the EU level** to ensure adequate data protection. The FD on data protection in the third pillar should be adopted as soon as possible and be applicable to data transfer to third countries.
- **Practical guidelines for some minimum-standards**: What data? Retention periods, limitations on access and further use, any derogations should be carried out restrictively and on a case-by-case basis

- **Proportionality** is a central issue when assessing PNR transfer: It is not sufficient for a measure to be *useful*, it must be *necessary* to achieve the purpose. The question should also be examined if there are other (less intrusive) ways to achieve the purpose.
- The issue of **transparency** was a re-occurring theme throughout the workshop: more evidence on the value of PNR would be helpful for establishing trust: many stakeholders (airlines, national and European Parliament) expressed the desire to be more involved in the process and to be properly informed.
- Mechanism are needed to **ensure guidelines are enforced**, i.e. independent monitoring of compliance
- **Joint Review of interim agreement** is an essential instrument before a new agreement can be concluded. Possibility of proposing a **permanent committee for joint review with participation of DPAs**
- Important for national **DPAs to liaise closely with national actors** (parliaments, governments, law enforcement).
- To find common ground, it is also necessary **to conduct a dialogue** in the broader sense, **at EU level with other stakeholders**, i.e. politicians, policymakers, law enforcement and the private sector (mainly airlines). Global approaches should also be found for example through co-operation with ICAO and IATA.
- **Communicating our underlying interests**, make visible why privacy matters and avoid too many technicalities. Make **public aware of these issues to gain support**
- Focus on **new agreement with US**, whilst taking into account the wider perspective of the strategy - could form the basis **for the approach to passenger data transfer generally**
- Combine current negotiations with other transatlantic dialogues in law enforcement to **include other security measures** (possibly also immigration) **as part of the agreement**. This would strengthen the EU's negotiating position
- The issue of PNR data should be made part of a wider framework to **include all passenger data**
- The new agreement should contain **clear and controllable obligations for all parties**. The airlines also have an interest in clarifying where their responsibility begins and ends.
- Data protection standards should evolve, new technological tools should be used to **keep step with latest technological development** (and hence the implications this can have for the data subject).

2 April 2007