Resolution on SWIFT, the PNR agreement and the transatlantic dialogue on these issues

2007/2503(RSP) - 14/02/2007 - Text adopted by Parliament, topical subjects

The European Parliament adopted a joint resolution from six political groups on SWIFT, the PNR agreement and the transatlantic dialogue on these issues, and stressed that, during the last few years, several agreements prompted by US requirements were adopted without the involvement of the European Parliament. Agreements on PNR, SWIFT and the existence of the US Automated Targeting System (ATS), have led to a situation of legal uncertainty with regard to the necessary data protection guarantees for data sharing and transfer between the EU and the US for the purposes of ensuring public security and, in particular, preventing and fighting terrorism. The solutions envisaged so far by the Council and the Commission as well as by private companies do not adequately protect the personal data of EU citizens.

Parliament welcomed the fact that the US administration had recently taken note of the reservations expressed by Congress and that it will seek to improve the situation by means of the following steps:

- the establishment of privacy officers and/or an independent privacy agency within the federal administration, who are to undertake privacy assessments of all initiatives that could potentially impinge on privacy;

- a mechanism to guarantee US citizens a right of appeal in the event of incorrect use of their data;

However, these improvements are insufficient as regards data protection for EU citizens. It would be warmly welcomed if the 1974 Privacy Act could also apply to EU citizens on a reciprocity basis in order for them to have access to their data, with a right of rectification and modification, as well as having access to a legal redress mechanism and to an independent data protection authority.

Parliament insisted that, in matters of data protection, the agreements should strive to achieve a high level of protection as regards risks of abuse and should be supplemented with binding principles at EU level as regards the protection of data for security purposes (third pillar). It was necessary to define with the US a common framework to safeguard the necessary guarantees that are needed in the special EU-US partnership in the fight against terrorism, which could also deal with all aspects concerning the free movement of persons between the EU and the US.

As regards the negotiation of the long-term PNR agreement: in addition to the points already adopted by Parliament its position of 27 September 2006, a future long-term PNR agreement should be founded on the following principles:

- evidence-based policy-making: a thorough evaluation must be carried out before a new agreement is concluded; the question of the effectiveness of the current agreement (and the previous one) should be addressed, as should the issue of the costs and competitiveness of European airline companies; the evaluation must address the implementation of the undertakings and the matter of PNR data in ATS;

transfers of PNR must be based on a clear purpose limitation principle;

- justification and proportionality: it would seem that in practice, for law enforcement and security purposes, Advance Passenger Information System (APIS) data are more than sufficient; these data are already collected in Europe in accordance with Council Regulation 2299/89/EEC on a code of conduct for computerized reservation systems, and may therefore be exchanged with the US under a comparable

regime; behaviour data in the PNR seem to be of limited use, as they cannot be identified if not linked to APIS; the justification for the general transfer of PNR data is therefore not satisfactory;

- a future agreement must be based on an adequacy finding with regard to the protection of personal data; from the EU side, it is clear that rules for the protection of personal data in the third pillar are urgently needed, as well as global standards covering all categories of personal data;

- there must be a regular evaluation of the programme's data protection adequacy and effectiveness, involving Parliament and, if possible, the US Congress; an annual evaluation must be part of any future agreement; the evaluation report must be made public, and must be submitted to the European Parliament;

- alternative solutions, such as the Electronic Travel Authorisations within a Visa Waiver Programme, instead of the transfer of PNR by airline companies, must equally comply with European data protection standards;

- the conditions currently laid down in the US undertakings must become an integral part of the agreement and must be legally binding; a future agreement must have more democratic legitimacy, with full involvement of the European Parliament and/or ratification by national parliaments;

- in any case, a future agreement must be based on the PUSH system and the PULL system should no longer be acceptable given that PUSH should already have been introduced under the previous agreement, as soon as it was technically feasible;

- passengers should be informed of the transfer of PNR records and have access to their data, including rectifying and modifying them, as well as having legal recourse to a legal mechanism or to an independent data protection authority;

As regards the access to SWIFT data: Parliament reiterated its concern over the fact that for four years, SWIFT, upon receipt of subpoenas, has been transferring to the US administration a subset of data treated in its US system, including data that did not concern US citizens and data not generated on US territory. It was very worrying that this situation, in breach of the Convention for the Protection of Human Rights and Fundamental Freedoms and the Charter of Fundamental Rights of the European Union, as well as of the Treaties and secondary legislation, has not been strongly criticised at an earlier stage either by the ECB or by the Group of 10 Central Banks that oversee SWIFT's activities, and that it is only recently that European banks and their customers have been made aware of the situation through press reports.

Parliament deeply regretted the fact that, several months after these matters came to light, the Council has not yet taken a stance on this subject affecting so many citizens, consumers and enterprises. Furthermore, only seven out of 27 Member States have responded to the questionnaire sent by the Commission to obtain clarification in relation to respect for national and Community data protection laws. MEPs repeated their concerns as regards the current system of supervision of SWIFT whose responsibility belongs to the Group of 10 Central Banks, with oversight by the ECB, but without formal competence. They called on the Council and the ECB to reflect together on the way to improve this system so as to ensure proper functioning of the alert process with full consequences in terms of action to be taken.

Parliament endorsed the opinion expressed by the EDPS on the role of the ECB and called on the ECB:

- as SWIFT overseer, to explore solutions in order to ensure compliance with data protection rules and to ensure that rules on confidentiality do not prevent information from being supplied in good time to the relevant authorities;

- as user of the SWIFTNet-Fin, to explore solutions to bring its payment operations into compliance with data protection legislation, and to prepare a report on measures taken no later than April 2007;

- as policymaker, to ensure, in cooperation with central banks and financial institutions, that European payment systems, including the updated system for wholesale payments "TARGET2", are fully compliant with European data protection law.

Parliament believed that the EU and the US are fundamental and loyal allies in the fight against terrorism. The legislative framework should be the basis for the negotiation of a possible international agreement, based on the assumption that SWIFT as a Belgian company is subject to Belgian law and is consequently responsible for the treatment of data in accordance with Article 4(1) of Directive 95/46/EC. The natural consequence would be for SWIFT to be obliged to stop its current practice of mirroring all data concerning EU citizens and enterprises in its US site or to move its alternative database site outside US jurisdiction. The international agreement must provide the necessary guarantees against abuse of data for economic and business purposes.

Parliament drew attention to the fact that SWIFT provides services elsewhere than in Europe and in the US and therefore considered that any measure adopted should take into account the global aspect of SWIFT's services.

Lastly, the House called on the Commission, which has competence both on data protection and on payment systems legislation, to analyse the potential for economic and business espionage stemming from the current design of payment systems in the broadest sense, thus including, in particular, messaging providers, and to report on ways of tackling the problem.