significant improvements. It restricts and clarifies the purposes for which the information may be used, such as serious transnational crimes and terrorism, and it establishes the time period for which data may be retained: after six months, the data must be depersonalised and masked. Should their data be misused, everyone has the right to administrative and judicial redress in accordance with US law. They also have the right to access their own PNR data and seek rectification by the US Department of Homeland Security, including the possibility of erasure, if the information is inaccurate.

The agreement, which entered into force on 1 July 2012, shall remain in force for seven years, until 2019.

In December 2011, the Council of the European Union approved the conclusion of an updated EU-Australia Agreement on the processing and transfer of PNR data.[240] The agreement between the EU and Australia on PNR data is a further step in the EU agenda, which includes global PNR guidelines,[241] setting up an EU-PNR scheme[242] and negotiating agreements with third countries.[243]

Financial messaging data

The Belgian-based Society for Worldwide Interbank Financial Telecommunication (SWIFT), which is the processor for most of the global money transfers from European banks, was operating with a mirror centre in the US and was confronted

240 Council Decision 2012/381/EU of 13 December 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, OJ 2012 L 186/3. The text of the Agreement, which replaced a previous 2008 agreement, is attached to this Decision, OJ 2012 L 186, pp. 4–16.

241 See in particular the Communication of the Commission of 21 September 2010 on the global approach to transfers of Passenger Name Record (PNR) data to third countries, COM(2010) 492 final, Brussels, 21 September 2010. See also Article 29 Working Group (2010), *Opinion 7/2010 on the European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries*, WP 178, Brussels November 12, 2010.

242 Proposal for a Directive of the European Parliament and of the Council on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, Brussels, 2 February 2011. In April 2011, the European Parliament requested FRA to provide an opinion on this Proposal and its compliance with the Charter of Fundamental Rights of the European Union. See: FRA (2011), *Opinion 1/2011 – Passenger Name Record*, Vienna, 14 June 2011.

243 The EU is negotiating a new PNR agreement with Canada, which will replace the 2006 agreement currently in force.

with the request to disclose data to the US Department of the Treasury for terrorism investigation purposes.[244]

From the EU perspective, there was no sufficient legal basis for disclosing these substantially European data, which were accessible in the United States only because one of SWIFT's data service-processing centres was located there.

A special agreement between the EU and the United States, known as the SWIFT Agreement, was concluded in 2010 to provide the necessary legal basis and to secure adequate data protection.[245]

Under this agreement, financial data stored by SWIFT continue to be provided to the US Treasury Department for the purpose of the prevention, investigation, detection, or prosecution of terrorism or terrorist financing. The US Treasury Department may request financial data from SWIFT, provided that the request:

- identifies as clearly as possible the financial data;
- clearly substantiates the necessity of the data;
- is tailored as narrowly as possible to minimise the amount of data requested;
- does not seek any data relating to the Single Euro Payments Area (SEPA).

Europol must receive a copy of each request by the US Treasury Department and verify whether or not the principles of the SWIFT Agreement are complied with.[246] If it is confirmed that they are, SWIFT must provide the financial data directly to the

244 See, in this context, Article 29 Working Party (2011), *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, WP 186, Brussels, 13 June 2011; Article 29 Working Party (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT)*, WP 128, Brussels, 22 November 2006; Belgium Commission for the protection of privacy (*Commission de la protection de la vie privée*) (2008), *'Control and recommendation procedure initiated with respect to the company SWIFT scrl'*, Decision, 9 December 2008.

245 Council Decision 2010/412/EU of 13 July 2010 on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, OJ 2010 L 195, pp. 3 and 4. The text of the Agreement is attached to this Decision, OJ 2010 L 195, pp. 5-14.

246 The Joint Supervisory Body of Europol has conducted audits on Europol's activities in this area, the results of which are available at: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

US Treasury Department. The department must store the financial data in a secure physical environment where they are accessed only by analysts investigating terrorism or its financing, and the financial data must not be interconnected with any other database. In general, financial data received from SWIFT shall be deleted no later than five years from receipt. Financial data which are relevant for specific investigations or prosecutions may be retained for as long as the data are necessary for these investigations or prosecutions.

The US Treasury Department may transfer information from the data received by SWIFT to specific law enforcement, public security or counter-terrorism authorities within or outside the United States exclusively for the investigation, detection, prevention or prosecution of terrorism and its financing. Where the onward transfer of financial data involves a citizen or resident of an EU Member State, any sharing of the data with the authorities of a third country is subject to the prior consent of the competent authorities of the concerned Member State. Exceptions may be made where the sharing of the data is essential for the prevention of an immediate and serious threat to public security.

Independent overseers, including a person appointed by the European Commission, monitor compliance with the principles of the SWIFT Agreement.

Data subjects have a right to obtain confirmation from the competent EU data protection authority that their personal data protection rights have been complied with. Data subjects also have the right to rectification, erasure or blocking of their data collected and stored by the US Treasury Department under the SWIFT Agreement. However, the access rights of data subjects may be subject to certain legal limitations. Where access is refused, the data subject must be informed in writing of the refusal and their right to seek administrative and judicial redress in the United States.

The SWIFT Agreement is valid for five years, until August 2015. It automatically extends for subsequent periods of one year unless one of the parties notifies the other, at least six months in advance, of its intention not to extend the agreement.