Prof. Dr. Gerrit Hornung, LL.M., Chair of Public Law, Information Technology Law and Legal Informatics, Universität Passau

Dr. Franziska Boehm, Centre for Security, Reliability and Trust (SnT), Université du Luxembourg

Comparative Study

on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security

–Passau/Luxembourg, 14 March 2012 –

The Greens | European Free Alliance
in the European Parliament

Comparative Study on the 2011 draft Agreement between the Unites States of America and the European Union on the use and transfer of Passenger Name Records (PNR) to the United States Department of Homeland Security

by Gerrit Hornung / Franziska Boehm

is licensed under a Creative Commons Attribution-ShareAlike 3.0 Unported License.

Contact to the authors:

Prof. Dr. Gerrit Hornung
Lehrstuhl für Öffentliches Recht, IT-Recht und Rechtsinformatik
Universität Passau
Innstr. 39
D-94032 Passau

Dr. Franziska Boehm
Université du Luxembourg
Interdisciplinary Centre for Security, Reliability and Trust (SnT)
Campus Kirchberg
6, rue Richard CoudenhoveKalergi
L-1359 Luxembourg

Funding for this study was provided by the Greens/EFA Group in the European Parliament.

Table of Contents

Executive summary ..... - 3 -
1 Introduction ..... - 5 -
2 Key problems and fundamental rights (brief overview) ..... - 6 -
2.1 Criticism and relevant arguments ..... - 6 -
2.2 "Accumulation" of surveillance measures and constraints from the Member States' Constitutions ..... - 8 -
3 Comparison between the different agreements (2004, 2007 and 2011) ..... - 9 -
3.1 Purpose and use of the data ..... - 9 -
3.2 Retention period ..... - 11 -
3.3 Transfer to third parties ..... - 12 -
3.4 Amount of data sets ..... - 14 -
3.5 Data subject's rights ..... - 15 -
3.6 Independence of supervision ..... - 15 -
3.7 Judicial review ..... - 16 -
4 Comparison between the provisions of the draft agreement and the draft Police and Justice Directive ..... - 18 -
5 Conclusions ..... - 19 -

Executive summary

This study compares the three PNR agreements: those of 2004 and 2007, as well as the current draft of 2011 matching them against the requests put forward by the European Parliament in its resolution of 5 May 2010 andthe proposal for a police and criminal justice data protection directive ofthe Commission of 25 January 2012. The outcomes of the analysis are briefly summarized in the following.

1. Purpose and use of the data have been extended

When comparing the 2004, 2007 and the 2011 agreements, the purposes for which the PNR data can be used have been considerably extended. According to Article 4 of the proposed agreement, PNR data can be used for other purposes not related to terrorist or related crimes (i.e. border control, use if ordered by a court, other violations of law). This extension is not in line with the demands of the European Parliament formulated in its resolution of 5 May 2010.

2. Retention period has been extended

The comparison of the data retention periods show that they were constantly extended until the current draft eventually abolished the time limit at all, bearing the risk of repersonalization after the "*anonymization*" envisaged after 15 years. The indefinite retention period (in particular for data of unsuspected individuals which have never been accessed) is, however, not in line with European data protection standards. The use of undefined terms such as "*anonymization*", "*masking out"* and "*repersonalization*" leads to uncertainty as regards the content of those terms.

3. Transfer to third parties has been broadened

Although some safeguards, including the information duty and express understandings incorporating data privacy protections, are contained in the 2011 agreement, the purpose of onward transfers is not particularly specified and not directly linked even to the very broad purposes mentioned in Article 4 (as it was in the former agreements by identifying the respective paragraph). Even if the purpose of transfer is linked to the overall purpose of the 2011 agreement, the justifications for transfers would nonetheless be wider than those of the former agreements as the provisions on purpose limitation in Article 4 have been extended.

4. Independence of supervision is still not guaranteed

The provisions regarding review and oversight have been clearly improved in the 2011 agreement. However, they are considerably weakened by the fact that there is no truly independent authority and indeed no mandatory oversight from outside the DHS at all. This is however, again not in line with European data protection standards.

5. Amount of data sets has not been reduced; less protection for sensitive data

There is no change or reduction of the data categories transferred to the U.S. since 2004. The already weakened protection for sensitive data from the 2007 agreement is further weakened in the 2011 draft.

6. Data subject's rightsand judicial review still not enforceable

Although the provisions on data subject's rights and on judicial review are more detailed than in the former agreements,it is doubtful whether the provisions of the agreement grant any new rights to EU citizens, in particular with regard to Article 21, stating that the agreement does

not confer any new right to individuals.In the other provisions, the proposal mostly refers to U.S. laws which would apply to the data subjects in any case. As according to the prevailing opinion, U.S. laws as such do not ensure an adequate level of data protection, the reference to U.S. law in force can hardly be deemed to ensure an adequate level of data protection (as stated in Article 19).

7. Comparison between the provisions of the draft agreement and the draft Police and Justice Data Protection Directive

The proposed agreement clearly does not comply with the standards of the proposed directive in many respects. Many of these shortcomings relate to the points mentioned before. Basic data protection standards are not respected. Provisions relating to the wide-ranging purposes, the very long retention period, the independency of supervision and the rights of individuals (access, correction, rectification, compensation) are far from being comparable to those of the draft police and criminal justice data protection directive. With regard to the adequacy standards in Article 34 of this proposal, it is barely understandable that Article 19 of the 2011 agreement states that DHS providesan adequate level of protection for PNR processing and use, “within the meaning of relevant EU data protection law”.

8. Conclusion

The draft 2011 PNR agreement, which is currently undergoing the consent procedure in the European Parliament, provides only very few improvements when compared to the 2004 and 2007 agreements and in some regards even lowers the data protection standards of the former agreements. Data transferred under the agreement can be used for purposes not related to terrorist and serious transnational crimes, retention periods have been extended, and data subject rights are still not enforceable. The draft 2011 agreement also clearly does not meet the data protection standards envisaged in the proposed directive on data protection in the field of police and criminal justice.

1 Introduction

The transfer of Passenger Name Record (PNR) data has been heavily discussed in recent years and appears to be a prototypic example of the conflicts between security interests and privacy fundamental rights which has evolved since the attacks of 11 September 2001.

As PNR data is usually collected by a controller which is based in an EU Member States, the respective national data protection laws apply in accordance with Article 4 (1) Directive 95/46. Companies are thus bound by both U.S. law and the law of the respective EU Member State. As the U.S. do not, as such, ensure an adequate level of protection as defined by Article 25 Directive 95/46, it is in principle, illegal for air carriers to transfer the data to the U.S. However, U.S. law precisely obliges the air carriers to do so. There is thus a conflict of law to which there was no solution prior to the respective PNR agreements. The first PNR agreement tried to solve this problem in 2004,[1] but it was squashed by the European Court of Justice due to the lack of a legal basis for the decision of the Council.[2] In July 2007, a follow-up agreement was signed.[3] In the absence of ratification, it has since only been applied provisionally. After the entry into force of the Treaty of Lisbon, the European Parliament was requested to give its consent. The Parliament did not do so, but instead called on the Commission to re-negotiate and substantially improve the agreement with regards to data protection standards in its resolution of 5 May 2010.[4] After negotiations with the U.S., the Commission initialed the agreement and recommended to the Council so sign it.[5] The Council adopted the agreement on 13 December 2011.

There are thus three succeeding PNR agreements: those of 2004 and 2007, as well as the current 2011 draft. As the Parliament had argued against the 2004 agreement, not only with regards to the lack of competence, but also in relation to the violations of fundamental rights, and requested in its resolution of 5 May 2010[6] that certain "minimum requirements" must be respected when exchanging PNR, it is of particular interest whether the current document improves the privacy and data protection rights of travelers.

This study thus aims at comparing the three documents and matching them against the requests put forward by the Parliament. To this end, we will first recall briefly the key problems of the PNR scheme with regard to fundamental rights and data protection laws. As the transfer of PNR data relates to the prevention, investigation, detection or prosecution of criminal offences, it is additionally important to compare the current PNR agreement to the

---

1 Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, OJ 2004, L 183/84 (in the following: the 2004 Agreement).

2 Both Article 95 and Article 300 TEC were not considered to be the appropriate basis, cf. ECJ, Joined Cases C-317/04 and C-318/04, European Parliament v Council and Commission; cf. Ulrich Ehricke, Thomas Becker and Daisy Walzel, "Übermittlung von Fluggastdaten in die USA", Recht der Datenverarbeitung 2006: 149-156; see also the case notes of Westphal, EuropäischeZeitschriftfürWirtschaftsrecht 2006: 406-407 and Peter Szczekalla, DeutschesVerwaltungsblatt 2006: 896-899.

3 Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ 2007, L 204/18 (in the following: the 2007 Agreement 2007).

4 European Parliament resolution of 5 May 2010 on the launch of negotiations for Passenger Name Record (PNR) agreements with the United States, Australia and Canada, final edition B7-0244/2010.

5 COM(2011) 807 final.

6 See above n. 4.

standards which the Union seeks to apply in this area in the future. The agreement will thus be assessed in the light of the proposal ofthe Commission of 25 January 2012.[7]

A careful analysis of the current PNR proposal is of particular importance in several respects. It relates to the protection of fundamental human rights (Articles 7 and 8 CFR, Article 8 ECHR, Article 16 TFEU), it could influence the proposed European PNR retention scheme[8] – but most of all, it could constitute a precedent for future data transfers to countries outside the European Union. According to Article 19 of the 2011 proposal, "*DHS shall be deemed to provide, within the meaning of relevant EU data protection law, an adequate level of protection for PNR processing and use*". It could therefore well be that other countries or other administrative branches in the U.S. will refer to the standards in the proposal in the future. The European legislative organs should keep this in mind when deciding upon the current draft.

2 Key problems and fundamental rights (brief overview)

The main concern expressed so far relate to the compatibility of the former as well as the current EU-U.S. PNR agreements with fundamental rights, in particular with data protection rights (above all with Articles 7 and 8 CFR, Article 8 ECHR, Article 16 TFEU). Various actors, such as the Article 29 Working Party, the Commissions' legal service, the Parliament, the EDPS[9] and academic literature[10] have already exhaustively elaborated on the main problems and concerns. The criticism mentioned in these articles and opinions is therefore only briefly illustrated in the following and restricted to the key points.

2.1 Criticism and relevant arguments

With regard to the mentioned fundamental rights, the PNR transfers must meet the requirements of necessity and proportionality. The key problem here is that the necessity of

---

[7] Cf. the proposal for a "Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", COM(2012) 10 final, 25 Jan 2012.

[8] See e.g. Boehm, "EU PNR: European Flight Passengers Under General Suspicion – The Envisaged European Model of Analyzing Flight Passenger Data", in: Computers, Privacy and Data Protection: an Element of Choice, eds. Serge Gutwirth, Yves Poullet, Paul De Hert, Springer 2011, p. 171-199;McGinley, "Die Verarbeitung von Fluggastdaten für Strafverfolgungszwecke", Datenschutz und Datensicherheit 2010: 250-253.

[9] Compare for instance: Opinion 7/2010 of the Article 29 Working Party, WP 178 (2010); Opinion of the EDPS of 9 December 2011 on the Proposal for a Council Decision on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, OJ C 35/03, 9.2.2012, see also draft recommendation of rapporteur Sophia in't Veld, 30 January 2012, 2011/0382 (NLE), Note from the Commission legal service to DG Home affairs of 18 May 2011; Letter from the Article 29 Working Party to the Members of the LIBE Committee of the European Parliament of 6 January 2012.

[10] Compare for instance: VagelisPapakonstantinou, and Paul De Hert, "The PNR Agreement and Transatlantic anti-terrorism Cooperation: No firm human rights framework on either side of the Atlantic," Common Market Law Review 46 (3) (2009): 885-919; Mario Mendez, "Passenger Name Record Agreement,European Court of Justice," European Constitutional Law Review 3 (2007): 127-147; Christian Schröder, "Der Zugriff der USA auf DateneuropäischerFlugpassagiere", Recht der Datenverarbeitung 2003: 285-290; Westphal (above n. 2); Franziska Boehm, "Datenschutz in der Europäischen Union", Juristische Arbeitsblätter 2009: 435-439; Waldemar Hummer, "Die SWIFT-Affaire. US-Terrorismusbekämpfung versus Datenschutz, Archiv des Völkerrechts 49 (2011), 203-245; Thomas Petri, "Unzulässige Vorratssammlungen nach dem Volkszählungsurteil? Die Speicherung von TK-Verkehrsdaten und Flugpassagierdaten", Datenschutz und Datensicherheit 2008: 729-732; Marina Tamm, "Rückwirkungen des gescheiterten SWIFT-Abkommens auf das Abkommen über Fluggastdaten?", Verbraucher und Recht 2010: 215-223.

the data transfer is continuously emphasized,[11] but remains unclear. So far it is doubtful whether the evidence offered is sufficient to demonstrate the necessity of the mass PNR transfer to the U.S.[12] As there has been offered no new evidence that the PNR analysis lead to arrests and eventually the conviction of terrorist and criminals with regard to the 2011 agreement, the criticism remains valid.

Extensive criticism also concerns the purpose and the use of the data. Up to now, none of the agreements have specified the exact purpose for which the PNR should be used. Whereas the initial idea was to use the PNR only for the prevention of serious crime and terrorism, all agreements included the possibility to use the PNR for other purposes (in particular for border purposes, possible profiling purposes, in court proceedings and for minor crimes). These additional uses have been the subject to criticism.[13]

In addition, the retention period has been exposed to critique since the first PNR agreement in 2004. It is criticized for being not proportional in relation to the purpose pursued. This is fostered when taking into account other PNR agreements, such as those with Canada and Australia, which provide for a much shorter retention period (Canada: 3,5 and Australia: 5,5 years). Compared to those, the U.S. retention period of up to 15 years seems to have been rather randomly chosen.[14]

Doubts have also been expressed in the context of the effective enforcement of access and redress possibilities for individuals.[15] As all of the agreements entailed a specific clause stipulating that the agreements shall not create any right or benefit under U.S. law,[16] the practical value of access and redress provisions have been called into question.[17] Doubts have concerned the question of whether adequate and effective access and redress possibilities in U.S. law exist and how these possibilities could be successfully used. Since the U.S. Privacy Act does not apply to EU citizens, it is doubtful whether the other U.S. statutes mentioned in the agreements (e.g. the FOIA) entail rights, which are comparable to those that would be available to EU citizens within the EU.

The provisions concerning domestic sharing and onward transfer have also triggered critical comments. Doubts with regards to the safeguards applied in this context and to the adequacy of the transfer are being discussed.[18] Further, the criticism refers to the lack of specification of the authorities entitled to receive PNR data.[19] In addition, it is criticized that the transfer to

---

[11] See e.g. COM(2011)807 final, p. 3 ("very important tool in the fight against terrorism and serious crime"), p. 6 ("a necessary tool that gives information that cannot beobtained by other means").

[12] Letter from the Article 29 Working Party to the Members of the LIBE Committee of the European Parliament of 6 January 2012;Opinion of the EDPS of 9 December 2011 (above n. 9), OJ C 35/03, 09.02.2012, p. 3; McGinley, (above n.8), p. 250 et seq.

[13] Compare note from the Commission legal service to DG Home affairs of 18 May 2011; Westphal (above n. 2), p. 407; Tamm (above n. 10), p. 222.

[14] McGinley, (above n.8), p. 250 et seq.; Westphal (above n. 2), p. 407; Ehricke, Becker and Walzel (above n. 2), p. 155; Tamm (above n. 10), p. 222.

[15] Tamm (above n. 10), p. 222; Boehm (above n. 10), p. 438; Westphal (above n. 2), p. 407.

[16] Compare Article 21 of the 2011 agreement.

[17] Compare letter from the Article 29 Working Party to the Members of the LIBE Committee of the European Parliament of 6 January 2012.

[18] Letter from the Article 29 Working Party to the Members of the LIBE Committee of the European Parliament of 6 January 2012.

[19] Opinion of the EDPS of 9 December 2011 (above n. 9), OJ C 35/03, 09.02.2012, p. 7.

third parties is not limited to acase-by-case basis and that thetransfers to third countries is not subject to prior judicial authorisation.[20]

Moreover, since the first EU-U.S. PNR agreement of 2004, the provisions on (independent) oversight have been criticized. Although Article 8 (3) CFR and the case law of the European Court of Justice[21] apply strict criteria to the independency of oversight, so far none of the agreements have complied with these requirements.[22]

With regard to the method of transmission, the use of the "pull" method (the U.S. authorities have direct access to the PNR of the airlines) instead of the "push" method (the airlines themselves transfer the data to U.S. authorities) has been heavily criticized.[23] Even though the 2007 agreement already obliged the air carriers to switch to the "push" method, this requirement was not implemented.[24] The 2011 agreement now provides for the use of the "push" method, but also allows for exemptions.

The large volume of transmitted data, including the possibility to transfer and process sensitive data, are a constant source of criticism.[25] In particular, as the wide ranging and therefore indefinite data categories required by the U.S. authorities[26] have not been modified since the first agreement of 2004, this criticism is not without merit.

2.2 "Accumulation" of surveillance measures and constraints from the Member States' Constitutions

It is worth mentioning that the EU-U.S. PNR agreement is but one element of a tendency to collect data of individuals never been suspected of having committed a crime.[27]In addition to the EU-U.S. PNR agreement, measures such as the data retention directive, the TFTP agreement and the planned EU-PNR system also target unsuspected individuals and are therefore subject to discussionin various Member States and at EU level.

The recent data retention judgment of the German Constitutional Court of 2 March 2010[28] addressed this accumulation of groundless surveillance measures and obliged the German legislature to consider theentirety of the already existing databases, if it plans to enact further data retention obligations. In other words, before individuals not suspected of wrongdoing are targeted by such measures, the German legislature is required to be very cautiouswhen enacting new measures. The scope for further groundless data retention obligations is therefore considerably reduced through the introduction of the data retention obligation in the telecommunications sector in Germany and vice-versa.

---

[20] Opinion of the EDPS of 9 December 2011 (above n. 9), OJ C 35/03, 09.02.2012, p. 7.

[21] C-518/07, Commission v. Germany of 9 March 2010.

[22] Compare draft recommendation of rapporteur Sophia in't Veld, 30 January 2012, 2011/0382 (NLE), paragraph 9; Boehm (above n. 10), p. 438.

[23] Compare for instance Petri (above n. 10), p. 729 et seq.

[24] Compare draft recommendation of rapporteur Sophia in't Veld, 30 January 2012, 2011/0382 (NLE), paragraph 5.

[25] Petri (above n. 10), p. 729 et seq. ; Schröder (above n. 10), p. 287; Ehricke, Becker and Walzel (above n. 2), p. 155.

[26] Martin Sebastian Haase, "Neues Abkommen zur Übermittlung von Fluggastdaten an die USA", ZD-Aktuell 2011, p. 128.

[27] CompareAntonie Knierim,"Kumulation von Datensammlungen auf Vorrat" Zeitschrift für Datenschutz 2011: 17-23.

[28] Judgment of the German Constitutional Court of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, cf. Gerrit Hornung and Christoph Schnabel, "Verfassungsrechtlich nicht schlechthin verboten. Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung", Deutsches Verwaltungsblatt 2010: 824-833.

Keeping the judgment of the German Constitutional Court in mind, another measure targeting individuals not suspected of criminal activity, such as the EU-U.S. PNR agreement, would possibly meet serious scrutiny at national level. Even if this judgment was clearly related to the legislation and constitutional constraints in Germany, the arguments of the German Constitutional Court emphasize that a new measure targeting unsuspected individuals must also comply with the constitutional restrictions of the Member States.

3 Comparison between the different agreements (2004, 2007 and 2011)

All articles without reference refer to the articles ofthe draft PNR Council Decision (2011).

3.1 Purpose and use of the data

Comparing the use and the purposes of the PNR in the different agreements, a constant expansion of the scope can be observed. The purpose of the original 2004 agreement was limited to the prevention and combat of terrorism and related crimes, other serious crimes (including organised crime) that are of transnational nature, and flight from warrants or custody for both groups of crimes.[29] The 2007 agreement extended these purposes to the protection of the vital interests of the data subject or other persons as well as to the use in any criminal judicial proceeding, or as otherwise required by law.[30]

These already far reaching purposes are again broadened in the draft PNR agreement of 2011. Article 4 is divided into 4 paragraphs which entail, on the one hand, a list of definitions of terrorist offences and related crimes (paragraph 1 (a)) and other transnational crimes punishable by a sentence of three years or more (paragraph 1 (b)), and on the other hand, further purposes PNR data may be used for (paragraphs 2 to 4). There is also the problem that domestic sharing in Article 16 is allowed on basically the same grounds. As Article 4 is drafted very broadly, so are the cases in which domestic sharing is legal.

Paragraph 1 (a) of Article 4 specifies the terms "*terrorist offences and related crimes*". A catalogue of examples is given. The use of the wording "*including conduct that* […]" when specifying these terms seems however, to indicate that this catalogue is not exhaustive and that the given definitions are only examples of several offences which may fall under the terms "*terrorist offences and related crimes*". As there is neither a definition of terrorism in the agreement nor in international law,[31] this leads to considerable legal uncertainty as regards the possible purposes.

Paragraph 1 (b) of Article 4 is structured in a similar way. The paragraph refers to "*other crimes that are punishable by a sentence of imprisonment by three years or more, and that are transnational in nature*". The paragraph also refers to a list of definitions which aims at specifying the criterion of "*transnational nature*". As in paragraph 1 (a) of Article 4, the use of the wording "*in particular*" when describing the criteria for transnational crime, also indicates that this list is not exhaustive and that further criteria may be used to classify a crime as transnational. Yet the list alone offers little guidance. According to paragraph 1 (b) (iv), it is sufficient that a crime "*is committed in one country but has substantial effects in another*

---

[29] Paragraph 3 of theUndertakings of the 2004 agreement, OJ 2004 L 235/11.

[30] Paragraph I, US letter to EU, annex to the 2007 agreement, OJ 2007 L 204/18.

[31] See e.g. Schmid"The Definition of Terrorism", in: The Routledge Handbook of Terrorism Research, 2011, pp. 39 et seq., available at http://books.google.com/books?id=_PXpFxKRsHgC&pg=PA39; see also the Report of the Ad HocCommittee established byGeneral Assembly resolution51/210 of 17 December 1996Sixth session (28 January-1 February 2002), available at http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N02/248/17/PDF/N0224817.pdf?OpenElement.

country". It appears that this could relate to any legal, economic, social or other effect. There is neither a definition of nor a mechanism to determine which effects qualify as "substantial", leading to the risk of diverse interpretation and legal uncertainty. Article 4 (1) (b) (v) even covers every crime committed in one country when the offender "*is in or intends to travel to another country*". From a literal reading, this would cover every business or holiday trip of the offender subsequent to the crime. The definition of transnational crime is thus very wide-ranging and not even limited to U.S. law enforcement.[32]From its wording, the DHS would for example be entitled to use the data to investigate a crime which relates to two European countries (i.e. is "transnational in nature") while not even touching the U.S. jurisdiction.

As there is no reference to a specific legal order (U.S., EU, Member States) regarding the minimum sentence, it is not clear which crimes are actually referred to. This raises the question of different applicable laws (with different minimum sentences), including concerns regarding the possibility of changing the applicable laws in the aftermath of the agreement. An exhaustive list would therfore avoid subsequent misunderstandings about the interpretation of offences and the use of PNR.[33]

Paragraph 2 of Article 4 further broadens the scope of the use of PNR ("*PNR may be used and processed on a case-by-case basis where necessary in view of a serious threat and for the protection of vital interests of any individual or if ordered by a court*."). As there is no indication that this paragraph has to be read together with the paragraph before (paragraph 1 of Article 4)it allows for the use of PNR for any purposes as long as this use is somehow ordered by a court.[34]This lack of substantive requirements opens the way to use the data in every case a court may find it useful.

Paragraph 3 of Article 4 additionally extends the purposes for which the PNR can be used. The identification of "*persons who would be subject to closer questioning or examination upon arrival to or departure from the United States or who may require further examination*" appears to include the use of PNR for a wide range of border control purposes. Recitals 3[35] and 14[36] underpin this assumption. This specific purpose is not necessarily related to the purposes mentioned in the other paragraphs of Article 4 and would considerably enlarge the use of PNR also with regard to the former agreements of 2004 and 2007 in which border purposes were not mentioned.

Paragraph 4 of Article 4 also constitutes a new provision in comparison to the former agreements. It states that "*Paragraphs 1, 2, and 3 shall be without prejudice to domestic law enforcement, judicial powers, or proceedings, where other violations of law or indications thereof are detected in the course of the use and processing of PNR*". The wording used in this paragraph does not clarify which "*other violations of law or indications thereof*" are actually meant. This leaves room for further interpretation with regard to the nature of these offences. It is for example not clear whether only criminal offences are included. The wording suggests however that this is not the case and accordingly, the data could be used in

---

[32] Compare also draft recommendation of rapporteur Sophia in't Veld, 30 January 2012, 2011/0382 (NLE), paragraph 2 which refers in this context to the comments of the Article 29Working Group and the EDPS.

[33] Compare in this regard: opinion of the EDPS of 9 December 2011 (above n. 9), OJ C 35/03, 09.02.2012, p.16.

[34] Compare also in this regard the draft recommendation of rapporteur Sophia in't Veld, 30 January 2012, 2011/0382 (NLE), the opinions of the Commission Legal Service, the EDPS and the Article 29 Working Party referred to in n. 9 above.

[35] "Recognizing the right and responsibility of states to […] protect their borders".

[36] "Further recognizing that the collection and analysis of PNR is necessary for DHS to carry out its border security mission […]".

proceedings on administrative offences or even breaches of ordinary civil law. With regard to criminal offences, paragraph 4 may render paragraph 1 (b) of Article 4 meaningless, as there is no mentioning of a minimum threshold for these violations (as opposed to paragraph 1 (b) of Article 4: sentence of three years or more).In consequence, the PNR could possibly be used for any other offences detected in the course of the use and processing of PNR.

Conclusion: When comparing the 2004, 2007 and the 2011 agreements, the purposes for which the PNR data can be used have been considerably extended. The single paragraphs of Article 4 (which define the purposes) seem to be not formally connected to each other. As a consequence, the mentioned purposes are not specifically linked to the overarching goal of the prevention, detection and investigation and prosecution of terrorist and related crime, which were subject to the former agreements. PNR data can be thus used for other purposes not related to terrorist or serious crimes (i.e. border control, use if ordered by a court, other violations of law). Taking into account the plethora of exceptions in Article 4 paragraph 2-4, the Commissions' statement that the purpose of processing is "*strictly limited to preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime*"[37] appears to be grossly misleading.

3.2 Retention period

Comparing the different agreements, a remarkable extension regarding the retention period can be observed. Whereas in the 2004 agreement the retention period was limited to 3.5 years (eight years only for the data which had been accessed during the first 3.5 years),[38] and the 2007 agreement allowed for an "active analytical database" for seven years and a "dormant, non-operational" one for additional eight years, the current proposal does not provide for a limit at all.

The PNR should stay in "*active database for up to five years"* whereby "*after the initial six months of this period, PNR shall be depersonalized and masked* […]".[39] After the five years, the PNR are "*transferred to a dormant database for a period of up to ten years*". There, the data can be "*repersonalized*" in "*connection with law enforcement operations*" in connection with "*an identifiable case, threat or risk*". Data collected for the purposes of Article 4 (1) (b) (transnational crimes that are punishable by a sentence of three years or more), should only be repersonalized for a period of up to five years. As there is in all these instances, the possibility of repersonalization, the data is in any case "personal data" in the meaning of Article 2 (a) of Directive 95/46/EC for the full period of fifteen years. The protection offered by the dormant database is additionally weakened by the fact that there are basically no substantive requirements for repersonalization, which may take place "in connection" with law enforcement operations (thus not even meeting the basic principle of necessity). The requirement of an identifiable case, threat or risk does not offer any guiding, as those three are alternatives and the "case" thus may mean any enquiry by any government official without being related to a threat or risk.

Following the dormant period, the data are not deleted, but "fully anonymized" without the possibility of repersonalization. (Article 8 (4)).However, data relating to a "*specific case or investigation may be retained in an active PNR database until the case or investigation is achieved*".[40] The change form "destruction" (2004) and "deletion" (2007) respectively to

---

[37] COM(2011)807 final, p. 3.

[38] Paragraph 15 of the Undertakings of the 2004 agreement, OJ 2004 L235/11.

[39] Article 8 of the 2011 agreement.

[40] Article 8 (5) of the 2011 agreement.

"anonymization" (2011) constitutes a shift to the disadvantage of the data subjects. If there was actually no possibility of repersonalization, then there would be no difference for the data subject's data protection rights. Experience has however, shown that the retention of large amounts of "anonymized" data over long periods of time bears the risk that it will eventually be possible to repersonalize it nonetheless. This will particularly relate to frequent travellers and those with unusual PNR data sets. To ensure the deleting of "*all data types which could serve to identify the passenger to whom PNR relate without the possibility of repersonalization*" in accordance with Article 8 (4), it will be necessary to delete a lot more data than just the name of the passenger. As there are no indications as regards the method to render the data "*fully anonymized*", it is unclear whether this will actually take place.

All in all, even if the PNR are never accessed or used, the retention period is infinite. While the data will be directly linked to the data subject for fifteen years, the risk of repersonalization remains even after this time. However, time limits for storing are essential in EU data protection law and must be taken into account to avoid indiscriminate storing of personal data in governmental databases.[41] The unlimited retention period seems to fail to strike the right balance between the rights of, in principle, unsuspected individuals and crime prevention interests, in particular with regard to the risk of the possible stigmatising effect the long-term data storage might have.

With regard to the use of the terms "depersonalization", "anonymization", "masking out" and "repersonalization", only the term "depersonalization" is further explained in the text. It refers to the "masking out" of certain fields of information entailed in the PNR, but not to all of them. Further criteria with regard to the "anonymization" or "repersonalization" are not given. Information, with regard to the technological feasibility of "anonymizing" or "depersonalizing" is also not offered.

Conclusion: A comparison of the retention periods between the 2004, 2007 and 2011 agreements shows that the time limit has been constantly extended until the current draft eventually abolished the time limit entirely. As the 2001 agreement explicitly states that the time frame for non-"anonymized" data will be reconsidered (Article 8 (6)) and the agreement will have to be re-negotiated after seven years (Article 26 (1)), there are also serious doubts whether data that would be collected under the 2011 proposal would actually be "anonymized" in the end. The indefinite retention period (in particular for data of unsuspected individuals which have never been accessed) is, however, not in line with European data protection standards.[42]The use of undefined terms such as "*anonymization*", "*masking out"* and "*repersonalization*" leads to uncertainty as regards the content of those terms.

3.3 Transfer to third parties

Transfer to third parties entails domestic data sharing and the onward transfer to third countries. The comparison between the agreements shows an extension of the actors allowed to receive PNR.

With regard to domestic data sharing, already in the 2004 agreement, the CBP (which is now a department of DHS and was the receiving partner at that time), was permitted to send data to other U.S. authorities, though only to authorities with counter terrorism or law enforcement

---

[41] ECtHR, *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04 from 4 December 2008, paragraph 119; ECtHR, *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00 from 6 June 2006, paragraphs 89-92.

[42] ECtHR, *S. and Marper v. the United Kingdom*, Application nos. 30562/04.

functions on a case by case basis.[43] Further provisions permitted the use "*for the protection of the vital interests of the data subject or of other persons*" (in particular regarding health risks) and "*the use or disclosure of PNR data in any criminal judicial proceedings or as otherwise required by law*".[44]

These very wide ranging purposes were further extended in the 2007 agreement to domestic transfer to authorities serving public security functions in support of "public security related cases (including threats, flights, individuals and routes of concern)".[45] Article 16 (1) (a) and (b) of the 2011 agreementnow refer to domestic authorities serving the wide ranging purposes of Article 4 of the agreement (analysed above), which include border security, the use of PNR if ordered by a court or other violations of law. In practice, the sharing with authorities pursuing the purposes of Article 4 would not lead to an improvement with regard to the plethora of domestic authorities authorized to receive PNR. The only substantive requirement for the transfer, apart from being somehow connected to the purposes of Article 4, relates to "*comparablesafeguards*" as set out in the agreement, which have to be respected in case of domestic data sharing (Article 16 (1) (d)).

Equivalent to domestic data sharing, the provisions on onward transfer have not been substantially changed. The 2004 as well as the 2007 agreement, involved data sharing with foreign government authorities with counter terrorism or law enforcement functions on a case by case basis,[46] as well as other purposes mentioned in the agreements (terrorism and related crime, other serious crime, organized crime, flight from warrants or custody for the mentioned crimes, includingthe protection of the vital interests of the data subject or other persons and the use in any criminal judicial proceeding).[47] A new clause was introduced in the 2007 agreement, requiring that data exchanges should only be carried out, apart from emergency circumstances, if"*express understandings*" between the third party and the DHS "*that incorporate data privacy protection comparable to*" those applied to the PNR by DHS were concluded beforehand.[48]

The 2011 agreement maintains this safeguard clause and introduces a new information duty. The competent authorities of the concerned Member State must now be informed, if the PNR of an EU citizen or resident is transferred to a third country. The purpose for which the data can be transmitted is, however, not particularly specified. As in the 2007 agreement, the purpose of transfer must be, in some way, linked to the overall purpose of the agreement, however not explicitly. Article 17 (1) states that PNR may be transferred "*only under terms consistent with this Agreement and only upon ascertaining that the recipient's intended use is consistent with these terms*" without clarifying what the term "*consistent with this Agreement*" means. In contrast to the provisions on domestic data sharing (Article 16), where direct reference to the purposes mentioned in Article 4 is made, this reference is lacking in Article 17. This missing reference, combined with the fact that the DHS itself ascertains whether (or not) the intended use is in accordance with the agreement, leaves a back door open for other possible transfer purposes.

As every transmission of personal data from one authority to another, including the subsequent use of such data, constitutes a separate interference with individual rights under

---

43 Paragraphs 28 et seq. of the Undertakings of the 2004 agreement, OJ 2004 L235/11.

44 Paragraphs 34 and 35 of the Undertakings of the 2004 agreement, OJ 2004 L235/11.

45 Paragraph II of the US letter to the EU, OJ 2007, L 204/21.

46 Paragraph 29 of the Undertakings of the 2004 agreement, OJ 2004 L235/11.

47 Compare paragraph II, US letter to EU, annex to the 2007 agreement, OJ 2007, L 204/21.

48 Paragraph II, US letter to EU, annex to the 2007 agreement.,OJ 2007, L 204/21.

Article 8 ECHR[49], the criteria applicable to the transfer and the subsequent use should be clearly defined.

Conclusion: Although some safeguards, including the information duty and express understandings incorporating data privacy protections, are entailed in the 2011 agreement, the purpose of onward transfers is not particularly specified and not directly linked even to the very broad purposes mentioned in Article 4. Compared to the former agreements (2004, 2007), in which the purpose of transfer was clearly linked to the purpose of the agreement (by identifying the respective paragraph), the 2011 agreement spares this clarification. Even if linking the purposes of transfer to the overall purpose of the 2011 agreement, the justifications for transfers would nonetheless be wider than those of the former agreements as the provisions on purpose limitation in Article 4 have been extended.[50]

3.4 Amount of data sets

The comparison between the different agreements with regard to the amount of data sets does not reveal any progress. The 2007 agreement seemed to reduce the transferred data sets from 34 (2004) to 19 (2007), but this reduction was rather a formal than a qualitative reduction, mainly because the same data sets have been summarized under fewer points than in the 2004 agreement. Point 14 of the 2007 agreement, for instance, entails information previously entailed in four different points (20, 22, 32 and 34) of the 2004 agreement. The 2011 agreement maintains the same 19 data categories as the 2007 agreement.

As regards sensitive data, the 2004 agreement stated that CBP would not use this type of information and would implement, with the least possible delay, an automated system, which filters and deletes it.[51] Both safeguards were watered down in 2007, when the automated filtering did not require immediate deleting of the data and the use of such data was admitted in exceptional case where the life of a data subject or of others could be imperilled or seriously impaired.[52] In such a case, the data was to be deleted within 30 daysonce the purpose for which it has been accessed is accomplished unless the further retention was required by law.

While the purpose (imperilment or impairment for the life of an individual) is maintained in Article 6 (3) of the 2011 proposal, the retention period is extended considerably. According to Article 6 (4), "*sensitive data shall be permanently deleted not later than 30 days from the last receipt of PNR containing such data by DHS*". Thus, sensitive data of passengers flying again within 30 days will be retained for an additional 30 days from the second flight, and in the case of frequent travellers, the data may not be deleted at all, without any further requirement. At least in these cases, the statement of the Commission that "sensitive data is […] deleted after a very short timeframe"[53]will not apply.

Additionally, Article 6 (4) allows "*sensitive data [to] be retained for the time specified in U.S. law for the purpose of a specific investigation, prosecution or enforcement action*", without referring to Article 6 (3). If read alone however, this sentence may be interpreted as to considerably broaden the use of sensitive data.

---

[49] The transmission enlarges the group of individuals with knowledge of the personal data and can therefore lead to investigations being instituted against the persons concerned,ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision from 29 June 2006, paragraph 79.

[50] See above chapter 3.1.

[51] Paragraph 9 et seq. of the Undertakings of the 2004 agreement.

[52] Paragraph III of the US letter to the EU, OJ 2007, L 204/21.

[53] COM(2011)807 final, p. 3.

Conclusion: There is no change or reduction of the data categories transferred to the U.S. since 2004. The weakened protection for sensitive data from the 2007 agreement is further weakened in 2011.

3.5 Data subject's rights

The Commission maintains that "individuals are provided with the right to access, correction, redress and information."[54] In the face of Article 21 (1), stating that the "*agreement shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public*",this is hardly true. Whatever the actual content of the proposed agreement is, it does not create any rights for persons or entities, which are not anyhow provided under U.S. law.

This impression is confirmed in the specific provisions. With regard to data security, Article 5 (5) states that "*the United States confirms that effective administrative, civil, and criminal enforcement measures are available under U.S. law for privacy incidents*", neither specifying these rights nor providing for additional remedies. The same applies to Article 10 (2), according to which "*DHS shall publish and provide to the EU for possible publication its procedures and modalities regarding access, correction or rectification, and redress procedures*", being silent on any substantive requirements as regards these rights.

Article 11 refers the data subject to the U.S. Freedom of Information Act. As in the 2004 and 2007 agreements, it is stated that according to this Act "*any individual, regardless of nationality, country of origin, or place of residence is entitled to request his or her PNR from DHS*". Article 11 (2) however also refers to the limitations under U.S. law and thus the provision does not change the legal situation at all.

Article 12 states that any individual may seek correction or rectification, but remains silent on the legal grounds such a claim may be based on. Even basic rules are missing, e.g. the obligation to erase data when the collection did not comply with the respective requirements or to correct it in case it is inaccurate. DHS is obliged to inform the individual of its decision, including the legal basis of a refusal and the options for seeking redress. A duty to specify the reasons for a refusal is however missing; it appears that it will be sufficient to simply state the legal basis.

Conclusion: At first sight, the enhanced level of detail appears to be a clear improvement of the 2011 proposal. An agreement which explicitly does not confer any new right to individuals (Article 21 (1)) can however, hardly be deemed to ensure an adequate level of data protection (as stated in Article 19). In other provisions, the proposal mostly refers to U.S. laws which would apply to the data subjects in any case. According to the prevailing opinion, U.S. laws as such do not ensure an adequate level of data protection,[55] and this situation is not substantially changed by the draft agreement.

3.6 Independence of supervision

With regard to independent oversight, a slight improvement in the 2011 agreement can be noted when compared to the former agreements. While in the 2004 as well as in the 2007 agreement, an oversight mechanism to protect privacy in the framework of the agreements was not mentioned (only redress possibilities), the 2011 agreement provides in Article 14 for "*independent review and oversight by Department Privacy Officers, such as the DHS Chief Privacy Officer*". Further, "*independent review and oversight*"shall be carried out by "*the DHS Office of Inspector General, the Government Accountability Office*[…] *and the U.S.*

---

[54] COM(2011)807 final, p. 3.

[55] Compare the list of general adequacy decisions of the Commission in which the U.S. are not included.

Congress". These "independent reviews" nonetheless do not correspond to the high standards the EU demands to fulfil the independence requirement in its case law.[56] All of the mentioned bodies (apart from the U.S. Congress) are not "*free from any external influence, including the direct or indirect influence of the state*" as required by EU case law and mentioned in Article 8 of the Charter of Fundamental Rights.[57] The bodies involved in the PNR processing, in particular those of the DHS, are, if at all, comparable to internal data protection officers, but such officers do not fulfil the independency requirement in EU law.

The Commission's states that the rules will be subject to review and oversight by the DHS Office of Inspector General, the Government Accountability Office "*and*" the U.S. Congress, suggesting that this applies cumulatively. In fact, Article 14 (2) provides for independent review and oversight "*by one or more of the following entities*". It will thus suffice under the 2011 agreement to subject its application to the review and oversight by the DHS itself alone, and it should therefore be stressed that there is no mandatory review and oversight from outside the DHS at all.

Conclusion: The provisions on review and oversight are a clear improvement of the 2011 agreement. However, they are considerably weakened by the fact that there is no truly independent authority and indeed, no mandatory oversight from outside the DHS at all.

3.7 Judicial review

Provisions on judicial redress are bound to the U.S. law in force in all of the agreements (2004, 2007 and 2011). As a consequence, a special redress procedure for EU citizens does not exist. However, all agreements mention the possibility to make requests based on the Freedom of Information Act (FOIA).[58] The 2004 as well as the 2007 agreement expressly mention concrete contact points to which such requests can be made. The 2007 agreement additionally mentions "*administrative Privacy Act protections*" being applicable to PNR, but this reference is abolished in the 2011 agreement.[59] However, in addition to the reference to the FOIA, Article 13 of the 2011 agreement mentions other relevant U.S. provisions (the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act and other provisions of U.S. law). According to this article, "*[a]ny individual regardless of nationality, country of origin or place of residence*" shall be entitled to "*seek effective administrative and judicial redress in accordance with U.S. law*". Further, if an individual believes that he/she has been delayed or prohibited from boarding because he/she was wrongly identified as a threat, the individual can complain by using the Traveler Redress Inquiry Program (DHS Trip) and are "*entitled to petition for judicial review in U.S. federal court from any final agency action by DHS relating to such concerns*".[60]

As Article 13 of the 2011 agreement refers back to U.S. laws as regards the redress for individuals, the provision appears to be a mere list of various U.S. laws which will apply without the PNR agreement. While it is thus questionable whether Article 13 confers any new rights to EU citizens[61] – apart from those they would nonetheless have, even without the

---

[56] C-518/07, Commission v. Germany of 9 March 2010.

[57] C-518/07, Commission v. Germany of 9 March 2010, paragraph 25.

[58] Paragraph 37 of the Undertakings of the 2004 agreement, paragraph IV, US letter to EU, annex to the 2007 agreement and Article 13 (3) (a) of the 2011 agreement.

[59] This is presumably mainly due to the fact that in 2010 PNR data were exempted from the Privacy Act and that the provisions of the Privacy Act are not applicable to EU citizens.

[60] Article 13 (4) of the 2011 agreement.

[61] Compare draft recommendation of rapporteur Sophia in't Veld, 30 January 2012, 2011/0382 (NLE), paragraph 9.

mentioning in the agreement – doubts were raised to what extend the mentioned rights are enforceable in practice.

The recent case *Hasbrouck v. U.S. Customs and Border Protection*[62] is the first U.S. case involving a PNR request made by a U.S. citizen. It includes some important findings to be mentioned in this context. Between 2007 and 2009, Mr. Hasbrouck, a travel journalist, made several requests to obtain information regarding his personal data, including PNR, held by the Customs and Border Protection (CBP, which is now a department of DHS). His requests were based on both the FOIA and the Privacy Act. As he received no response to any of his requests, he filed an appeal in each of the cases. Only after these appeals were filed, the CBP agreed to meet and revealed – more than three years after the first request was made – some of the information (including some redacted excerpts from PNR[63]) held by them in 2009. None of the information received was however considered to be complete by Mr. Hasbrouck. Information regarding the possible transfer to other authorities, for instance, remained concealed.

Although the request of Mr. Hasbrouck was based on both the FOIA and the Privacy Act, the information he eventually received was limited to the FOIA requests, because, since a change in the applicable law in 2010, PNR have been exempted from the provisions of the Privacy Act.[64] The case thus shows that it is possible to receive some information on PNR based on the FOIA, but this information does not entail a complete overview of all the information stored by the authorities. As there are no provisions in the FOIA giving individuals a right to know with which third parties/authorities their PNR are shared, it seems unlikely that information in this regard will be provided. This however contradicts EU data protection law which provides for information of individuals about the onward transfer of their personal data.[65]

The three years delay in processing Mr. Hasbrouck's request, the fact that he received only some restricted information after he filed the claim before a court and the exemption of the PNR from the Privacy Act give rise to doubts as to whether requests of EU citizens will be treated more carefully. If even U.S. citizens meet serious difficulties in enforcing their rights and the agreement expressly stipulates that it does not confer "any right or benefit" under U.S. law to EU citizens, serious doubts with regard to the practical enforceability remain.

Conclusion: Provisions on judicial review are based on the respective U.S. law in force in all of the agreements (2004, 2007 and 2011).It is thus doubtful whether the provisions of the agreement grant any new rights to EU citizens, in particular with regard to Article 21, which expressly states that "*This agreement shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public*". With regard to the practical enforceability

---

62 *Edward Hasbrouck v. U.S. Customs and Border Protection*, United States District Court for the Northern District of California, San Francisco Division, order, No. 10-3793 RS.

63 The information received included data about his travel movements, including data about a train transfer between Brussels and Paris, as well as data to inspections at borders (e.g. his shoes were cleaned and disinfected, an apple was seized), see: http://hasbrouck.org/blog/archives/001607.html#example.

64 The reason that his request based on the Privacy Act was dismissed was the result of a change of applicable law in 2010 which exempted PNR data from the Privacy Act, compare:*Edward Hasbrouck v. U.S. Customs and Border Protection*, United States District Court for the Northern District of California, San Francisco Division, order, No. 10-3793 RS, p. 3-5 and http://www.papersplease.org/wp/wp-content/uploads/2010/02/ats-exemptions-dhs-2009-0055-0001.pdf.

65 Compare Article 12 (1) Directive 95/46: "recipients or categories of recipients" and Article 12 (1) (c) of the draft Directive, COM(2012)10 final: "the recipients or categories of recipients to whom the personal data have been disclosed, in particular the recipients in third countries".

of the provisions of the agreement, doubts remain as to whether U.S. authorities comply as stated in the agreement in a timely manner with the requests of EU citizens.

4 Comparison between the provisions of the draft agreement and the draft Police and Justice Directive

A closer look at the proposal of the Commission of 25 January 2012[66] is useful in two respects. First, even if still subject to deliberations in and negotiations between the European Parliament and the Council, the proposal clearly demonstrates the evolved standards of the Union for data processing and data transfers in the area of police and justice. Second, the 2011 PNR proposal should already be assessed with regard to the adequacy rules of the proposed directive, because the agreement will operate in practice after the entering into force of the new European data protection instruments.

With regard to the former, the proposed 2011 PNR agreement clearly falls short of the standards of the proposed directive in many respects. Many of these shortcomings relate to the points analysed in Chapter 3. The very wide and unclearly formulated purposes[67] can hardly be described as "*specified, explicit and legitimate purposes*" as required by Article 4 (b) of the proposed directive. The very long retention periods and the use of unclear terms such as depersonalization and masking[68] contradict the standards of Article 4 (e), according to which data forms must permit identification of data subjects for no longer than it is necessary for the purposes for which the personal data are processed. Further, there is no attempt to distinguish between different categories of data subjects, as envisaged in Article 5 of the proposed directive. Article 7 of the 2011 agreement states that the U.S. shall not make decisions that produce significant adverse actions affecting the legal interests of individuals based solely on automated processing and use "*of PNR*". At least in a literal reading, this would permit such decisions when they are based on data, which include PNR and other additional data, contravening Article 9 (automated decisions) of the proposed directive.

While the rules on transparency in Article 10 of the 2011 agreement relate to Articles 10 and 11 of the proposed directive, Article 11 of the agreement includes an access right, which is however not comparable to the right of access as provided for in Article 12 of the proposed directive. Even setting aside the apparent problems of enforcement of a FOIA claim to PNR data even for U.S. nationals[69] and the restrictions in U.S. laws to which Article 11 of the agreement refers to,[70] it should be stressed that Article 12 (1) of the proposed directive requires the controller to provide a greater amount of information than only the PNR as such, if the individual makes a request for access.

As regards correction and rectification rights, even basic rules are missing in Article 12 (1) of the 2011 agreement. Examples are the obligation to rectify data that is inaccurate and to erase data when the collection did not comply with the respective requirements (as provided for in Articles 15 and 16 of the proposed directive).

The rules on data security in Article 5 of the 2011 agreement are, albeit not providing the same degree of details, comparable to Article 27 to 29 of the proposed directive, with the

---

66 Proposal for a Directive on the protection of individuals with regard to the processing of personal data bycompetent authorities for the purposes of prevention, investigation, detection orprosecution of criminal offences or the execution of criminal penalties, and the freemovement of such data, COM(2012)10 final.

67 See abovechapter3.1.

68 See above chapter 3.2.

69 See above chapter 3.7.

70 See above chapter 3.5.

exception of informing a supervisory authority in cases of privacy breaches (Article 5 (4) mentions the "*relevant European authorities*", without referring to national supervisory authorities or the EDPS). This leads to one of the greatest discrepancies, namely the absence of any mandatory review and oversight from outside the DHS, which contradicts the compulsory rules on supervisory authorities in Articles 39 to 43, including their duties and powers in Articles 44 to 47 of the proposed directive. There is thus also no right to lodge a complaint with a supervisory authority (Article 50 of the proposed directive). With regard to the rules on liability and the right to compensation (Article 54 of the proposed directive), it is noticeable that the words "liability", "damage", "compensation" and "responsibility" do not even appear in the 2011 agreement, which simply refers individuals to U.S. laws.[71]

As Article 19 of the 2011 proposal states that DHS shall be deemed to provide, "*within the meaning of relevant EU data protection law*", an adequate level of protection for PNR processing and use, it is worth mentioning that the proposed directive significantly specifies these adequacy rules in Article 34.[72] The elements to be considered in the future are, according to Article 34 (2):

a) the rule of law, relevant legislation in force, both general and sectoral, including concerning public security, defence, national security and criminal law as well as the security measures which are complied with in that country or by that international organisation; as well as effective and enforceable rights including effective administrative and judicial redress for data subjects, in particular for those data subjects residing in the Union whose personal data are being transferred;

b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, for assisting and advising the data subject in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States; and

c) the international commitments the third country or international organisation in question has entered into.

In all three respects, the proposed agreement reveals considerable weakness. This relates (a) to the problem of the lack of enforceable rights,[73] which are apparently not even effective for U.S. citizens.[74] Element (b) must be seen as completely missing, as there is no mandatory independent supervisory authority at all, not to mention the further requirements as regard its role. Considering the plethora of problems described in chapter 3, point (c) regarding international commitments in the proposed agreement, finally appears to be rather weak. All in all, it is hardly possible to describe the 2011 proposal as meeting the adequacy criteria of Article 34 of the proposed directive.

5 Conclusions

While the current proposal provides for some minor improvements when compared to the former two versions (e.g. the slight improvements regarding the conditions for onward transfer), the main privacy and data protection problems of the agreement, mentioned in chapter 2, remain unsolved. In some cases, the level of data protection is even watered down

[71] See above chapter 3.5.

[72] Cf. Article 25 Directive 95/46/EC.

[73] See above chapter 3.5.

[74] See above chapter 3.7.

(e.g. almost no purpose limitation, no time-limit for data retention etc.). When comparing the 2011 draft agreement to the demands of the European Parliament in its resolution of 5 May 2010, it appears that those concerns are not addressed in the proposal.

Possibly, the most striking example relates to the wide-ranging purposes for which the PNR may be used. The Parliament clearly demanded a limitation of the purposes,[75] which is not complied with. In this context, there is, for instance, no mention of the instruments the Parliament proposed to take as a reference instruments (Framework Decision 2002/475/JHA on combating terrorism or the Framework Decision 2002/584/JHA on the European Arrest Warrant) to limit the use of the PNR.

Further, the Parliament asked for an international agreement with the status of a legislative act in order to provide necessary safeguards for EU citizens when concluding the agreement.[76] Nonetheless, the current draft explicitly states in its Article 21 that "*This agreement shall not create or confer, under U.S. law, any right or benefit on any person or entity, private or public*".

Another requirement which is not met by the current draft, relates to the missing privacy impact assessment. Other instruments and possible less intrusive methods have not been evaluated before proposing the current draft as demanded by the Parliament.[77]

In addition, the requested independent review is not guaranteed. This is one of the most important reasons why the standards of the agreement are not in line with European data protection standards (other examples are: the non-respect of purpose limitation, proportionality and the length of storage periods). With regards to the use of the data, it is not limited to specific crimes or threats on a case-by-case basis as required by the Parliament[78]

The conditions for transfer of PNR to third countries have slightly improved when compared to the former agreement but do not yet comply with the requirements the Parliament demanded in its resolution of 2010. The express understandings between the third party and the DHS "*that incorporate data privacy protection comparable to*" those applied to the PNR by DHS (Article 17 (2) of the 2011 Agreement), are not comparable to "specific adequacy findings" the Parliament asked for in its resolution. Further, there are still exemptions concerning the use of the push method when transferring PNR data to the US. This also contradicts the Parliament's demands.

All in all, the current agreement does neither improve the data protection standards of the 2004 and 2007 agreements nor lead to a coherent approach on PNRs. It is thus not at all in line with the requirements set by the European Parliament in its PNR resolution of 5 May 2010.

If the European Parliament would consequently reject the proposed PNR agreement, the legal situation would be similar to the one before the agreements were concluded.[79] Air carries would be in the rather complex situation of either violating U.S. or EU law,[80]but such conflicts of law appear in other areas as well when there are diverse regulatory approaches.

---

[75] European Parliament resolution of 5 May 2010 (above n. 6), final edition B7-0244/2010, paragraph 9 (a).

[76] European Parliament resolution of 5 May 2010 (above n. 6), final edition B7-0244/2010, paragraph 2.

[77] European Parliament resolution of 5 May 2010 (above n. 6), final edition B7-0244/2010, paragraph 5.

[78] European Parliament resolution of 5 May 2010 (above n. 6), final edition B7-0244/2010, paragraph 9 (c).

[79] This holds true in the absence of bilateral agreements which could follow from a rejection. The content of such agreements cannot be predicted here and would depend on the constitutional constraints (as well as the negotiating power) of the Member States; see for the German example above chapter 2.2.

[80] See chapter 1.

Data subjects would lose the protection provided by the 2011 draft: the provisions on purposes, data security, data transfer, retention periods, oversight, data subject's rights and judicial review would not apply. The analysis in chapter 3 has however shown that most of these rules provide little protection anyway. Others (such as data security measures) can be expected to be enforced without any PNR agreement, as the U.S. administration has a clear self-interest in that respect. Regarding the rights of the individuals, most provisions of the 2011 agreements are either in lack of substantial requirements or refer to U.S. law which would apply (or not) to the PNR data anyway. It thus appears that a rejection of the proposal would not considerably lower the data protection of EU citizens with regard to the use of PNR data, while sticking to its constitutional obligation to protect the fundamental rights of Union citizens as well as promoting these rights in its external affairs.