

# **THE REGULATION OF REGISTERED TRAVELLER PROGRAMMES**

Wouter Oude Alink

Leiden University Law School

31 July 2013

## TABLE OF CONTENTS

List of Abbreviations	4
Introduction	5
Chapter 1: Registered Traveller Programmes	7
1.1 Context	7
1.2 What is a Registered Traveller Programme?	7
1.3 Biometric data	8
1.4 Points of concern	9
1.5 RTPs as a commercial tool	10
1.6 Conclusions Chapter 1	10
Chapter 2: International Legal Framework	11
2.1 Chicago Convention	11
2.2 ICAO Annex 9 Facilitation	12
2.2.1 SARPs on Customs	13
2.2.2 SARPs on Security	14
2.2.3 SARPs on Travel documents	14
2.3 ICAO Annex 17 Security	14
2.3.1 SARPs on Unlawful interference	15
2.3.2 SARPs on National organization and appropriate authority	15
2.3.3 SARPs on Security procedures	16
2.4 Legal force of Standards and Recommended Practices	16
2.5 Conclusions Chapter 2	17
Chapter 3: European Legal Framework	19
3.1 Regulation 562/2006	19
3.2 Regulation 300/2008, as amended by Regulation 18/2010	23
3.2.1 Regulation 300/2008	23
3.2.2 Regulation 18/2010	24
3.3 Regulation 185/2010, as amended by Regulation 173/2012	24
3.3.1 Regulation 185/2010	25
3.3.2 Regulation 173/2012	25
3.4 Regulation 1077/2011	26
3.5 Conclusions Chapter 3	26
Chapter 4: Existing Registered Traveller Programmes in the Netherlands and the United States	28
4.1 The relevance of national law	28
4.2 The Netherlands	28

4.3	United States	30
4.3.1	Registered Traveller Programmes in the U.S.	30
4.3.2	Registered Traveller Programmes under U.S. Law	31
4.4	Conclusions Chapter 4	33
Chapter 5: The Proposal for an RTP Regulation in the European Union		34
5.1	Proposal for a Regulation establishing a Registered Traveller Programme	34
5.1.1	Objectives	34
5.1.2	Characteristics	34
5.1.3	Legal elements	35
5.2	Conclusions Chapter 5	35
Chapter 6: Legal issues of Registered Traveller Programmes		37
6.1	Aviation security standards	37
6.2	The status of the RTP smart card or token	37
6.3	Issues of liability	38
6.4	Privacy rights and data protection	38
6.5	Conclusions Chapter 6	40
Conclusions and recommendations		41
List of Sources		43

## **LIST OF ABBREVIATIONS**

API	Advance Passenger Information
CBP	United States Customs and Border Protection
EEA	European Economic Area
EU	European Union
ICAO	International Civil Aviation Organization
MRTD	Machine Readable Travel Documents
RTP	Registered Traveller Programme
SARPs	Standards and Recommended Practices
SIS	Schengen Information System
TFEU	Treaty on the Functioning of the European Union
TSA	Transportation Security Administration
U.S.	United States
VIS	Visa Information System

## INTRODUCTION

Already in the 1990s research concluded that one of the main annoyances passengers experienced when travelling by air were the long queues for customs at airports and the amount of time it takes to get through customs. At the same time research showed that the more time passengers have to spend at the airport after they have gone through customs, waiting to board the plane, the more money they tend to spend.<sup>1</sup> Back then it led to the awareness and desire to find ways to reduce handling times at border control, especially in the light of the continuous growth of passenger air transport worldwide. One way to deal with this problem is by introducing a Registered Traveller Programme [hereafter: RTP], which has been done so far on a relatively small scale. Examples are Privium at Amsterdam Schiphol Airport, the Netherlands, and Global Entry at U.S. airports. An RTP is a programme whereby a passenger provide personal details, such as passport data and address details, in combination with biometric data for security reasons (*pre-screening and vetting*), to the RTP, which enables him to have quick border passing. Since subscription to an RTP may well involve some costs, it is mostly attractive for frequent travelers.

As said, there are few existing Registered Traveller Programmes. In this thesis I will discuss those in The Netherlands and the United States. In the European Union, a Proposal for a Regulation establishing a Registered Traveller Programme has been submitted in February 2013, dealing with an RTP for third country travelers passing the *Schengen*-borders.

The establishment of an RTP touches upon and involves various aspects of air law and regulations, such as the Chicago Convention and ICAO standards, aviation security law, airport law but also privacy law. Furthermore there is international law playing a role, as well as EU law (in the EU), and national laws. The establishment of an RTP may also involve adaptation of existing legislation.

In this thesis I want to study the legal implications of Registered Traveller Programmes – the central research question is thus as follows: **“What are the legal issues of Registered Traveller Programmes and how to address them?”**

In order to answer this question, I will go into the following sub-questions:

In the first chapter I will answer the question “what is a Registered Traveller Programme?” I think it is important to start with this question, because the term needs to be defined first, in order to be able to talk about the legal issues of RTPs. In order to answer this question various definitions will be discussed as they are found in the EU proposal for a Registered Traveller Programme, in the national laws of the Netherlands and the United States and in various background documents and articles on

---

<sup>1</sup> Piera, A., *The Simplifying Passenger Travel Programme and its Legal Implications*, in: *Air & Space Law*, Vol. 28(3), 2003, pp. 132-138

the subject. I will also go into the different roles that the various involved parties – the State, airports, airlines, private companies – have in an RTP.

The following topic to be addressed is the regulatory and legal framework in which RTPs are operable. Therefore in chapter 2 and 3 the Chicago Convention, the relevant ICAO Annexes and existing EU legislation will be discussed. Legal provisions as well as standards and practices will be discussed.

Narrowing down to the national level, in chapter 4 I will go into existing Registered Traveller Programmes, that is in The Netherlands, and in the United States, and I will answer the questions “what do these RTPs entail?”, and “under which laws do they function?”.

In chapter 5 I go back to the regional level and address the EU proposal for a Regulation establishing Registered Traveller Programme for third country travelers. The sub-question here is “How has the EU addressed the RTP?”, and the proposed regulation will be compared to the existing RTPs in the Netherlands and the U.S..

In the Chapters 2-5 I will have identified the relevant legal issues of RTPs on an international, EU and national level. In Chapter 6 I will address the various issues comprehensively. These issues include: aviation security standards, the status of the RTP smart card or token, issues of liability, and privacy rights and data protection. Issues regarding passenger name record and advanced passenger information, as well as discrimination issues will also be addressed.

The abovementioned questions and the research involved will enable me to finish this paper with conclusions answering the central research question, that is identifying the legal issues and come up with solutions and/or recommendations how to address them.

## **CHAPTER 1: REGISTERED TRAVELLER PROGRAMMES**

### **1.1 Context**

Year after year, international civil air passenger traffic is growing. To mention a few examples, the number of air passengers – domestic and international – carried by air carriers registered in the following respective States between 2008-2012, in Australia rose from 54.5 to 65.2 million passengers, in Brazil from 58.8 to 94.6 million passengers, in China from 191.0 to 318.5 million passengers, in Germany from 107.9 to 110.6 million passengers and in the United States from 701.8 to 736.6 million passengers<sup>2</sup> – despite the economic crisis during these years. This ever growing number of air traffic has consequences for the air traffic related activities on the ground at airports, such as baggage handling, airport facilities, security control and border control: in the end either capacity needs to be expanded in order to be able to deal with more passengers, or things need to be done more efficiently.

As mentioned in the Introduction, waiting time for customs and the amount of time it takes to get through customs is a main annoyance for passengers. How much more convenient would it be if this time could be reduced without compromising the quality of border control.

A solution has been found at the end of the 20<sup>th</sup> century in the development of Registered Traveller Programmes: whereas Privium was developed in the years 1998-2001, so before the 9/11 attacks, and therefore seemingly more commercial driven, the RTPs in the United States and the EU proposal focus more on efficient border control and safeguarding security, the latter two also being government-driven.

### **1.2 What is a Registered Traveller Programme?**

In a Registered Traveller Programme [hereinafter: RTP], a passenger has applied for entering this programme. The applicant is then being screened and interviewed to establish that there are no security concerns. His biometric data are taken, which are then either stored on a token or in a central database. The passenger can now pass customs when entering or exiting a State through an automated gate where his biometric data are checked and compared with the ones stored on the token or in the central database – depending of the technical system behind the programme.

In the EU Proposal for a Regulation establishing a Registered Traveller Programme it is defined as follows:

In practice the RTP would work at the border the following way: A registered traveller would be issued a token in the form of a machine-readable card containing only a unique

---

<sup>2</sup> (<http://data.worldbank.org/indicator/IS.AIR.PSGR>), last visited (6 July 2013)

identifier (i.e. application number), which is swiped on arrival and departure at the border using an automated gate. The gate would read the token and the travel document (and visa sticker number, if applicable) and the fingerprints of the travelers, which would be compared to the ones stored in the Central Repository and other databases, including the Visa Information system (VIS) for visa holders. If all checks are successful, the traveller is able to pass through the automated gate.<sup>3</sup>

As will be shown in chapter 4, a central database is not a necessity per sé for a functioning RTP.

Apart from expected higher revenues for the airport operator, an RTP has two big advantages:

- 1) For the passenger participating in an RTP because he spends less time waiting in queues and going through customs; and
- 2) Passengers participating in an RTP have been pre-vetted and have been judged to be no security risk; therefore the border control authorities can concentrate their resources to detect the individuals that possibly do constitute a risk.

An RTP is especially attractive for frequent travellers, who can by participating save a lot of waiting time at airports. As may be clear, participation is on a voluntary basis and normally requires a fee.

An RTP is not the same as a security check! Whether or not a passenger takes part in an RTP, he still needs to be checked for not carrying forbidden items and liquids with him.<sup>4</sup>

### **1.3 Biometric data**

Biometric data are physiological data of a person that makes him uniquely identifiable. Examples of biometric data that are or can be used for RTPs are fingerprints, iris-recognition, and facial recognition.

For the use in an RTP these biometric data need to be converted in a number or code and then stored in an automated repository or database in such a way that these can be compared with the actual features.<sup>5 6</sup>

As will be elaborated in chapter 5, in the EU proposal for a Regulation establishing an RTP indeed a central repository will be put in place. Alternatively, another method is the use of a smart card, whereby the biometric information is stored on a card itself, instead of in a central database. An

---

<sup>3</sup> Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, COM(2013) 97 final, Brussels, 28.2.2013, p. 3

<sup>4</sup> Cf. Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security, OJ L 55, 5.3.2010, p. 12: 4.1 *Screening of passengers and cabin baggage*

<sup>5</sup> Abeyratne, R., *Aviation Security Law*, Springer 2010, p. 111

<sup>6</sup> Haas, E., *Back to the Future? The Use of Biometrics, its Impact on Airport Security, and how this Technology Should Be Governed*, in: *Journal of Air Law and Commerce*, Vol. 69(2), 2004, pp. 459-489



example of an RTP using the smart card is *Privium*, the RTP of Amsterdam Schiphol Airport, which RTP will be addressed in chapter 4. Since the biometric information is being kept on the smart card, there is no need to have a centrally maintained database as well. This smart card ensures that passengers can be accurately identified by means of biometric verification without the need for further validation, reducing the time needed for going through customs.<sup>7</sup>

As mentioned at the beginning of this subchapter, several biometric data are being applied for the use in RTPs. The Netherlands' *Privium*, the UK's *Iris Recognition Immigration System (IRIS)*, Indonesia's *Saphire* and Germany's *Automated Border Control (ABC)* use iris recognition, whereas Australia's *SmartGate* and Portugal's *ID* scheme use face recognition technology; the UAE's *e-gate* uses fingerprints, and Israel's Ben Gurion Airport Authority is even using hand geometry.<sup>8</sup>

#### **1.4 Points of concern**

The usefulness of the biometric information is determined by the operator's ability and efficiency to organise, apply and access it. In the center of the system is the database or smartcard that contains the biometric information for comparison to identify the individual. In order to control the invasiveness and use of the acquired biometric information, it is important to distinguish between publicly and privately maintained databases.<sup>9</sup> This comes together with the need to be aware of possible privacy issues and data protection legislation in various jurisdictions as well as "the liability of the database manager that might emerge pursuant to a breakdown of the database or inaccuracy of information produced as a result of data-matching, which in turn might lead to inconsistencies in the identification process."<sup>10</sup> These issues will further addressed in chapters 4 and 6.

Another issue, of a technical nature, is the fact that technology is evolving rapidly – keeping up-to-date will be a continuous necessity, not in the least because of vulnerability when a system is easy to decode, particularly when data are stored centrally in a database.<sup>11</sup> As has become clear in recent times, IT systems of governments and commercial enterprises such as banks are under constant threat of being attacked by hackers.<sup>12</sup>

For the introduction of an RTP several parties are involved: 1) the State, in its role of legislator and performing its duty of border control and safeguarding security, 2) the airport, which may be State

---

<sup>7</sup> *Supra*, note 6

<sup>8</sup> Lockie, M. (ed.), *RTPs keep the world moving*, in: *Biometric Technology Today*, Vol. 16(7-8), 2008, pp. 10-11

<sup>9</sup> *Supra*, note 6

<sup>10</sup> *Supra*, note 5, at p. 112

<sup>11</sup> *Id.*

<sup>12</sup> See for example: (<http://www.reuters.com/article/2013/05/18/us-cyber-summit-banks-idUSBRE94G0ZP20130518>), last visited (6 July 2013)

owned and controlled, corporatised or privatised, and 3) one or more private companies, for the technicalities of the RTP IT-system.

### **1.5 RTPs as a commercial tool**

As RTPs are not mandatory for air passengers, but are offered as an alternative *next to* the existing ‘normal’ way of going through customs at airports, they can be offered as a commercial product. For example *Privium* offers three types of memberships, for different fees, each offering different services, such as – beside the fast border passage –: priority parking, a discount at Schiphol Airport valet parking, and business class check-in with participating airlines, to name a few.<sup>13</sup>

While the development and implementation of an RTP is also commercially driven and taking place on a local level, there are no widely internationally accepted standards yet for RTPs, as compared to eVisas and ePassports to which international standards apply, such as those of ICAO Doc 9303 on ePassports.<sup>14 15</sup>

This seems to imply that a smart card or token issued under an RTP is not considered to be a travel document as such, as opposed to a ‘real’ passport or visa. The status of the RTP smart card or token will further be addressed in chapter 6.2.

### **1.6 Conclusions Chapter 1**

While the motive for the adoption of a Registered Traveller Programme at first was commercially driven and provided as an extra service to the passenger, if so desired to be complemented with additional services, later on the safeguarding of aviation security became an important motive. In both cases also the improvement and speeding-up of the border control process played an important role.

With regards to the technical details it is possible to adopt RTPs with and without a central database. However, under all circumstances keeping up with technical developments is a principle requirement in order to ensure the protection of the system and recorded data. Another condition is that for all parties involved, rights, obligations and responsibilities are clearly defined. How this is done in practice will be explained in chapter 4 and 5.

---

<sup>13</sup> (<http://www.schiphol.nl/Reizigers/OpSchiphol/Privium.htm>), last visited (6 July 2013)

<sup>14</sup> Lockie, M.(ed.), *Registered travel – just another document?*, in: *Biometric Technology Today*, Vol. 15(10), 2007, pp. 8-10

<sup>15</sup> ICAO Doc 9303 Machine Readable Travel Documents, Part 3, Vol. 2, 3<sup>rd</sup> edition, 2008

## CHAPTER 2: INTERNATIONAL LEGAL FRAMEWORK

As indicated in the Introduction, the adoption of an RTP involves various aspects of air law and related regulations, in the field of aviation security law, airport regulations, privacy law and data protection.

With regards to the international legal framework, relevant to the scope of this thesis are the 1944 Chicago Convention on International Civil Aviation<sup>16</sup> [hereafter: Chicago Convention] and its Annexes 9 and 17.

### **2.1 Chicago Convention**

Currently 191 States are Party<sup>17</sup> to the Chicago Convention, which dates from 1944. It is therefore safe to say that the Chicago Convention has worldwide applicability.

The Chicago Convention is an international treaty that forms the basis for the regulation of international civil aviation.

At the time of the drafting of this document, the drafters could probably not have foreseen the technical developments that would lead to the introduction of RTPs. However in the Chicago Convention we can find a number of articles that are of relevance for this thesis, because they address issues of security, the application of international standards and practices.

The first article is Article 13, which addresses *Entry and clearance regulations*. According to Article 13 domestic rules apply to the entry and exit of passengers to and from the territory of a State with regards to immigration, passport and customs regulations. Article 13 therefore provides contracting States with the liberty to enact regulations in these fields, such as an RTP.

The next relevant article is Article 22, on the *Facilitation of formalities*: through Article 22, States are encouraged to come up with measures that “prevent unnecessary delays” to passengers, especially when it comes to immigration and customs regulations. Again, in my view this can be seen as an inducement to implement an RTP.

The third relevant article is Article 23, dealing with *Customs and immigration procedures*. In my opinion, Article 23 leaves room for States for differing levels of application: the obligation for States to establish procedures only applies for as far as a State finds it practicable. So apparently when a State deems a practice not practicable it does not need to adopt it. The reason behind this may have been the fact that this article is about practices to be established or recommended in the future, that is after

---

<sup>16</sup> Chicago Convention on International Civil Aviation 1944, 15 UNTS 296-361 (1948)

<sup>17</sup> ([http://www.icao.int/secretariat/legal/List%20of%20Parties/Chicago\\_EN.pdf](http://www.icao.int/secretariat/legal/List%20of%20Parties/Chicago_EN.pdf)), last visited (7 July 2013)

the entry into force of the Chicago Convention. Since it is very unlikely for any State to be willing to be bound by provisions that have not been drafted yet, it has been a necessity to provide for optionality in this article.

For the establishment of RTPs this article means that if they may become an established or recommended practice, a State may very well adopt an RTP, but even when the opposite would be the case, a State could still adopt an RTP when finding it not practicable not to do so.

Article 37 addresses the *Adoption of international standards and procedures* and explicitly mentions the role of the International Civil Aviation Organization [hereafter: ICAO] in ensuring global uniformity in regulations, standards, procedures, and organization of civil aviation related matters. This article can be advantageous as well as disadvantageous for the development of RTPs, since its only goal is uniformity. This can be the adoption of RTPs worldwide, maybe even through standardised practices, in which case it is advantageous, but it can also exclude the adoption of RTPs, which would make the implementation of an RTP in a single State a deviation from existing practice. Obviously, since RTPs are still the exception to the rule worldwide, they do deviate from the existing practices – whether or not defined as a ‘practice’ as in an ICAO Annex – of border control at airports.

In conjunction with Article 37 there is Article 38 dealing with *Departures from international standards and procedures* according to which it is not obligatory for a State to comply with international standards or procedures when it considers them “impracticable”. The question arising from this article is: “What is meant exactly by impracticable?” This is not defined, and therefore leaves room to a State to deviate from existing practice as long as it notifies ICAO.

The last article of relevance is Article 54(l), on the functions of the ICAO Council: article 54 reconfirms the task of ICAO to establish standards and practices. It adds that these standards and recommended practices are laid down in Annexes to the Chicago Convention. The Chicago Convention currently has 18 Annexes, of which hereafter I will discuss two in the context of this thesis.

## **2.2 ICAO Annex 9 Facilitation**

The first Annex to discuss is *Annex 9 to the Convention on International Civil Aviation on Facilitation*<sup>18</sup> – [hereafter: Annex 9]. First of all there is the definitions of a travel document:

Travel Document: A passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.<sup>19</sup>

---

<sup>18</sup> ICAO Annex 9 *Facilitation*, 12<sup>th</sup> ed., July 2005 [hereafter Annex 9]

In other words a travel document can be a passport, visa or *something else!* A travel document on its turn is defined as a passport or *other official documentation of identity, for the purpose of international travel.* According to this definition one could argue that a smart card issued in the framework of an RTP is a travel document. However this would be in contradiction with what I stated in chapter 1.5. It also depends of the question in so far as a smart card or token can be considered ‘an official documentation of identity.’ To give an example: the Privium smart card is issued by Schiphol, which is a private company, therefore in my view it can hardly be considered an *official* document of identity. Furthermore, ICAO Doc 9303 distinguishes between machine readable passports and machine readable travel documents, and provides standards for both.<sup>20</sup> In chapter 1.5 however I have mentioned that there are no international standards for RTPs yet, as opposed to passports and visas, seeming to imply that a RTP smart card has a different status. The issue of the status of an RTP smart card or token will be dealt with below in chapter 6.2.

### 2.2.1 SARPs on Customs

With regards to the scope of this thesis, Annex 9 provides Standards and Recommended Practices [hereafter: SARPs] in three relevant fields, that is customs, security, and travel documents.

Concerning customs, Contracting States have to provide an expeditious processing of passengers and efficient customs services.<sup>21</sup> Furthermore, provided services and facilities need to be “flexible and capable of expansion to meet traffic growth.”<sup>22</sup>

The clearance of passengers should be arranged under border control regulations in such a way that unnecessary delays are prevented.<sup>23</sup> More specifically, at international airports of considerable size – how big exactly is not specified – applicable technology and a multi-channel immigration inspection system or other means of streaming passengers should be adopted.<sup>24</sup> As a Recommended Practice Annex 9 sets a goal of not more than forty-five minutes for the clearance of passengers disembarking an aircraft, under normal circumstances.<sup>25</sup>

These provisions in my view all support the adoption of an RTP; it promotes efficiency, time savings and the use of technology, while at the same it expands capacity of customs services.

---

<sup>19</sup> *Supra*, note 18 at p. 1-3

<sup>20</sup> Doc 9303 – Machine Readable Travel Documents, 2005/2006/2008; Supplement to Doc 9303, 4 April 2013

<sup>21</sup> *Supra*, note 18, at p. 6-1

<sup>22</sup> *Id.*, at p. 6-1

<sup>23</sup> *Id.*, at p. 3-1

<sup>24</sup> *Id.*, at p. 3-3

<sup>25</sup> *Id.*, at p. 3-3

### **2.2.2 SARPs on Security**

In general, facilities and services provided at international airports must be able in terms of flexibility and capacity to deal with an increase in security requirements arising from increased threat.<sup>26</sup> When aiming at an efficient application of border controls on passengers through the development of procedures, Contracting States must take into account aviation security.<sup>27</sup> Lastly, for the facilitation of aircraft departure it is recommended that screening and examination techniques for the examination of passengers are efficient.

So the SARPs on security aim at efficiency, without compromising on security. In my view, for the development of an RTP this is not necessarily a hindrance, but an important requirement not to overlook.

### **2.2.3 SARPs on Travel documents**

One standard goes as far as to provide that Contracting States “shall establish controls on the creation and issuance of travel documents in order to safeguard against the theft of their stocks and the misappropriation of newly issued travel documents,”<sup>28</sup> a requirement that is not that much aviation specific, but rather general. Is a smart card or token issued under an RTP considered to be a travel document, then this provision is relevant as it puts the issuance of these under control of the State.

Also, Contracting States are obliged to keep the security features in their travel documents up-to-date, with the aim of preventing fraud and misuse.<sup>29</sup>

Recommended practices are to issue travel documents as machine readable travel documents [hereafter: MRTDs]<sup>30</sup> and to incorporate biometric data in their MRTDs,<sup>31</sup> a practice being in line with the development of RTPs.

## **2.3 ICAO Annex 17 Security**

In Annex 17 to the Convention on International Civil Aviation on Security<sup>32</sup> [hereafter: Annex 17], we find the following relevant definitions and SARPs, which I have categorized in three groups:

---

<sup>26</sup> *Supra*, note 18, at p. 6-1

<sup>27</sup> *Id.*, at p. 3-1

<sup>28</sup> *Id.*, at p. 3-8

<sup>29</sup> *Id.*, at p. 3-7

<sup>30</sup> *Id.*, at p. 3-11

<sup>31</sup> *Id.*, at p. 3-9

<sup>32</sup> ICAO Annex 17 *Security*, 8<sup>th</sup> ed., April 2006

SARPs on unlawful interference; SARPs on national organization and appropriate authority; and SARPs on security procedures.

### **2.3.1 SARPs on Unlawful interference**

According to Annex 17, the main goal in all matters relating to safeguarding civil aviation against acts of unlawful interference is the safety of passengers, crew, ground personnel and the general public. In order to safeguard civil aviation against acts of unlawful interference, regulations, practices and procedures need to be adopted by each Contracting State. For the same purpose in each Contracting State an organization needs to be established. This organization, and the regulations, practices and procedures shall:<sup>33</sup>

- a) protect the safety of passengers, crew, ground personnel and the general public in all matters related to safeguarding against acts of unlawful interference with civil aviation;
- and b) are capable of responding rapidly to meet any increased security threat.<sup>34</sup>

For the adoption of an RTP this means that the above must be taken into account; the implementation of an RTP cannot in any way be detrimental to security. The system of pre-vetting RTP participants must be waterproof in order to comply with these Standards.

### **2.3.2 SARPs on National organization and appropriate authority**

Each Contracting State must adopt a national civil aviation security programme to “safeguard civil aviation operations against acts of unlawful interference, through regulations, practices and procedures which take into account the safety, regularity and efficiency of flights.”<sup>35</sup> For the development, implementation and maintenance of such a programme, each Contracting State shall designate an appropriate authority.<sup>36</sup> This authority must “define and allocate tasks and coordinate activities between the departments, agencies and other organizations of the State, airport and aircraft operators and other entities concerned with or responsible for the implementation of various aspects of the national civil aviation security programme.”<sup>37</sup>

Next to a national civil aviation security programme, airports serving civil aviation in Contracting States must also have their own airport security programme, meeting the requirements of the national

---

<sup>33</sup> *Supra*, note 32, at p. 2-1

<sup>34</sup> *Id.*, at p. 2-1

<sup>35</sup> *Id.*, at p. 3-1

<sup>36</sup> *Id.*, at p. 3-1

<sup>37</sup> *Id.*, at p. 3-1

civil aviation security programme. An authority at these airports must be responsible for the coordination of implementation of security controls.<sup>38</sup>

### **2.3.3 SARPs on Security procedures**

On security procedures we find the recommended practices that Contracting States should, whenever possible, arrange that the interference with and delay to security controls and procedures of civil aviation is a minimal as possible, provided that the effectiveness of the security controls and procedures is not compromised.<sup>39</sup> Furthermore, the development of new security equipment, processes and procedures for better achievement of civil aviation security objectives should be promoted.<sup>40</sup>

Both Annex 9 and Annex 17 do not define into detail the goals and measures which need to be ensured. They do not provide for quantifiable standards, so how these goals are met and how measures are been given form is for the Contracting States to decide upon and fill in.

## **2.4 Legal force of Standards and Recommended Practices**

The terms ‘standards’ and ‘recommended practices’ are not defined in the Chicago Convention. For a definition we have to look at the ICAO Assembly Resolutions, more precisely in Resolution A36-13:<sup>41</sup>

Standard – any specification for physical characteristics, configuration, material, performance, personnel or procedure, the uniform application of which is recognized as necessary for the safety or regularity of air navigation and to which Contracting States will conform in accordance with the Convention; in the event of impossibility of compliance, notification to the Council is compulsory under Article 38 of the Convention;

Recommended Practice – any specification for physical characteristics, configuration, material, performance, personnel or procedure, the uniform application of which is recognized as desirable in the interest of safety, regularity or efficiency of international air navigation and to which Contracting States will endeavor to conform in accordance with the Convention.

---

<sup>38</sup> *Supra*, note 32, at p. 3-1

<sup>39</sup> *Id.*, at p. 2-1

<sup>40</sup> *Id.*, at p. 2-2

<sup>41</sup> Resolution A36-13: *Consolidated Statement of ICAO policies and associated practices related specifically to air navigation*, in Doc 9902, *Assembly Resolutions in Force* (as of 28 September 2007) at II-3. See also: ICAO Doc 7670 *Resolutions and Recommendations of the Assembly 1st to 9th Sessions (1947-1955)*, Montreal, Canada, 1956, Assembly Resolution A1-31 “Definition of International Standards and Recommended Practices”, now consolidated into Resolution A36-13



As mentioned under 2.1.1, in Article 37 of the Chicago Convention it is established that ICAO adopts standards and practices. In doing so, ICAO is not limited by said Article in the range of subjects it addresses.<sup>42</sup> An example is ‘security’, which is a topic that is not explicitly mentioned in Article 37, but as demonstrated under 2.1.2 and 2.1.3 ICAO has indeed issued standards and recommended practices in this field. According to the same Article, States “undertake to collaborate in securing the highest practicable degree of uniformity”. Therefore, especially when read in conjunction with Article 38, the adoption of standards is not an obligation. Contracting States are only obliged to *notify* ICAO if they choose *not* to comply with the standards because they find it impracticable.<sup>43</sup> States have, however, committed themselves to strive for the highest practicable degree of uniformity, and, as Michael Milde puts it: “States are strongly motivated to implement international standards by the sheer realities of international life: non-compliance with SARPs could eliminate the State concerned from any meaningful participation in international air navigation and air transport.”<sup>44</sup>

Moreover, Article 54(l) of the Chicago Convention confirms that SARPs do not form an integral part of said Convention, but they are *designated as Annexes* to the Convention. Therefore they also do not have the same legal force as the Convention, in the sense that they do not constitute hard law.<sup>45</sup> In line with article 37 and 38, non-compliance with SARPs does not constitute a violation of the Chicago Convention – only non-notification of non-compliance is a violation.<sup>46</sup>

Even though Article 90 of the Chicago Convention speaks of the ‘coming into force’ of the Annexes, by its wording – ‘recommended’ – and its definition – adoption is ‘desirable’, a recommended practice as laid down in an Annex cannot be compulsory in nature, and clearly has a less peremptory status than a standard. In line with Article 38, Contracting States only need to notify ICAO of non-compliance of standards, and not in case they do not comply with recommended practices.<sup>47</sup>

## **2.5 Conclusions Chapter 2**

Neither in the Chicago Convention, nor in its Annexes do we find any mentioning or clear referral to Registered Traveller Programmes. This does not mean that there are no provisions in these documents that are relevant for the adoption of RTPs. In the Chicago Convention there are a number of Articles on regulation, procedures and facilitation that must be taken into account for the implementation of an RTP. The same goes for the standards and recommended practices of the ICAO Annexes. Even

---

<sup>42</sup> Milde, M., *International Air Law and ICAO (Essential Air and Space Law 4)*, Eleven International Publishing, 2008, p. 159

<sup>43</sup> *Id.*, p. 159

<sup>44</sup> *Id.*, p. 161

<sup>45</sup> *Id.*, p. 158

<sup>46</sup> Abeyratne, R., *Aviation Security Law*, Springer 2010, p. 273

<sup>47</sup> Dr. Jiefang Huang, *Aviation Safety and ICAO* (Doctoral Thesis Leiden University), Kluwer Law International/E.M. Meijers Institute for Legal Research, 2009, p. 62

though there are no provisions in either the Chicago Convention or in the Annexes forbidding RTPs, they do provide for issues that have to be taken into account, such as efficiency, uniformity and security.

A special case is the legal force of the standards and recommend practices which as such are not mandatory, but States Party to the Chicago Convention must notify ICAO when they do not comply with the standards. In reality, States will be inclined however to follow the ICAO standards in order to be able to participate in international civil aviation.

## CHAPTER 3: EUROPEAN LEGAL FRAMEWORK

In this Chapter I will address the relevant EU legislation, that is Regulation 562/2006 – with reference to the Charter of Fundamental Rights of the European Union –, Regulation 300/2008, as amended by Regulation 18/2010, Regulation 185/2010, as amended by Regulation 173/2012 and Regulation 1077/2011. Regulation 45/2001 and Directive 95/46 will be dealt with in chapters 5 and 6 respectively, because of their close connection to the subjects discussed in these chapters.

### **3.1 Regulation 562/2006**

Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 [hereafter: Regulation 562/2006] establishes a Community Code on the rules governing the movement of persons across the external borders of the Member States of the European Union, and is also called the Schengen Borders Code.<sup>48</sup> This Regulation formulates common rules for the border control at the Schengen borders, while within the Schengen area persons can move freely without having to pass internal border controls. This Regulation is relevant for the scope of this thesis while the EU has recently communicated a proposal for a new Regulation concerning an RTP for third country travellers passing the Schengen borders.

In its Preamble, Regulation 562/2006 emphasize the importance of border control for security:

(8) Border control comprises not only checks on persons at border crossing points and surveillance between these border crossing points, but also an analysis of the risks for internal security and analysis of the threats that may affect the security of external borders. It is therefore necessary to lay down the conditions, criteria and detailed rules governing checks at border crossing points and surveillance.

The way border control is approached, executed or maintained therefore has its effect on national or regional security.

However, it also provides:

(9) Provision should be made for relaxing checks at external borders in the event of exceptional and unforeseeable circumstances in order to avoid excessive waiting time at borders crossing-points. The systematic stamping of the documents of third-country

---

<sup>48</sup> Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 105, 13.4.2006

nationals remains an obligation in the event of border checks being relaxed. Stamping makes it possible to establish, with certainty, the date on which, and where, the border was crossed, without establishing in all cases that all required travel document control measures have been carried out.

In my opinion, this first sentence seems to represent a very odd way of reasoning: when it gets very busy at the border then security is less important?! This is followed by a stamping obligation that under no circumstances can be relaxed. The importance of (9) for RTPs is twofold:

- 1- The application of an RTP would reduce border crossing time, reducing the need to relax checks at busy times; and
- 2- By use of an RTP, the ‘physical’ stamping can be replaced by ‘electronic stamping’, that is scanning of the RTP-token.

The last point from the Preamble is:

(20) This Regulation respects fundamental rights and observes the principles recognized in particular by the Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union has been referred to, because according to Article 8 of this Charter everyone has the right to the protection of his or her personal data. Furthermore these personal data must be processed fairly, for specified purposes, and based on the consent of the person concerned or if provided by law. Each person has the right to access collected data that concern him or her, and also has the right to have these data rectified. An independent authority must see on the compliance with these rules.<sup>49</sup> The Charter itself is aimed at the EU and its institutions, bodies, offices, etcetera, and the Member States for as far they are implementing EU law. The Charter also says that its principles “*may be implemented by legislative and executive acts taken by institutions, bodies and offices and agencies of the Union, and by acts of Member States when they are implementing Union law,*”<sup>50</sup> herewith implying that its principles as such are not enforceable.

Article 5 of Regulation 562/2006 states the entry conditions for third-country nationals, for stays not exceeding three months per six-month period. Necessary requirements are:

- a valid travel document or equivalent
- a valid visa or required

---

<sup>49</sup> Charter of Fundamental Rights of the European Union, OJ 2010 C83/02

<sup>50</sup> *Id.*, Article 52(5)

- justifiable purpose and conditions of intended stay as well as sufficient means of subsistence, or being in the position to acquire such means lawfully

Furthermore no alert should have been issued in the Schengen Information System [hereafter: SIS] for the purpose of refusing entry to the third-country national, nor should the third-country national be considered to be a threat to public policy, internal security, public health or the international relations of any of the Member States.

Article 7 provides that “cross-border movement at external borders, shall be subject to checks by border guards.” A distinction is being made between a minimum check for all persons and a thorough check for third-country nationals.

The single purpose of a minimum check is to establish a person’s identity on the basis of his travel document(s). The verification is “rapid and straightforward”, “where appropriate by using technical devices and by consulting, in the relevant databases, information exclusively on stolen, misappropriated, lost and invalidated documents, of the validity of the document authorizing the legitimate holder to cross the border and of the presence of signs of falsification or counterfeiting.”<sup>51</sup>

Third-country nationals shall undergo thorough checks. On entry and/or exit, these include the verification of the conditions laid down in Article 5, and, where applicable, of documents authorizing residence and the pursuit of a professional activity. In addition, the following aspects, partly duplicating those of Article 5, are covered:

- a) verification that the third-country national is in possession of a document which is valid for crossing the border and which has not expired, and that the document is accompanied, if applicable, by the required visa or residence permit;
- b) verification of the travel document for signs of falsification or counterfeiting;
- c) examination of the entry and exit stamps on the travel document of the third-country national concerned, in order to verify, by comparing the dates of entry and exit, that the person has not exceeded the maximum duration of authorised stay in the territory of the Member States;
- d) verification regarding the point of departure and the destination of the third-country national concerned and the purpose of the intended stay;
- e) verification that the third-country national concerned has sufficient means of subsistence for the duration and purpose of the intended stay, for his or her return to the country of origin or transit to a third country into which he or she is certain to be admitted, or that he or she is in a position to acquire such means lawfully;

---

<sup>51</sup> *Supra*, note 48, Article 7(2)

- f) verification that the third-country national concerned, his or her means of transport and the objects he or she is transporting are not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States. Such verification shall include direct consultation of the data and alerts on persons and, where necessary, objects included in the SIS and in national data files and the action to be performed, if any, as a result of an alert.<sup>52</sup>

I have listed these conditions so extensively, to show all the aspects that need to be taken into account for the adoption of an RTP for the Schengen borders, and may be affected if not. It also mentions the criteria that can be included in a RTP central database or on a RTP token, as a timesaving measure. Secondly, it shows that a distinction need to be made between frequent travellers who most of the time cross the border for the same reason, and infrequent travellers who cross the border for various reasons. Based on the Articles 5 and 7 of Regulation 562, the first group constitutes a target group for an RTP, while the resources that are then saved can be used for border checks on the latter group which requires more thorough examination.

Article 9 provides that separate lanes at the border crossings are allowed. It distinguishes between a lane for EU/EEA/CH citizens and a lane for all other citizens.<sup>53</sup> In line with this article I do not see an immediate objections against a third lane for third-country nationals participating in an RTP.

Article 10 deals with the stamping of the travel documents of third-country nationals, which shall be systematically stamped on entry and exit, and distinguishes three different kinds of documents to be stamped:

- (a) the documents, bearing a valid visa, enabling third-country nationals to cross the border;
- (b) the documents enabling third-country nationals to whom a visa is issued at the border by a Member State to cross the border;
- (c) the documents enabling third-country nationals not subject to a visa requirement to cross the border.<sup>54</sup>

For the adoption of an RTP this means that on the RTP smart card or token these three different groups need to be recognizable for 'e-stamping', that is these data need to be verifiable when this smart card or token is being scanned.

---

<sup>52</sup> *Supra*, note 48, Article 7(3)

<sup>53</sup> *Id.*, Article 9

<sup>54</sup> *Id.*, Article 10

### **3.2 Regulation 300/2008, as amended by Regulation 18/2010**

Regulation (EC) no 300/2008 on common rules in the field of aviation security was amended by Regulation 18/2010 on national quality control programmes in the field of aviation security. The most relevant provisions of these two Regulations are highlighted and discussed in the two following subchapters.

#### **3.2.1 Regulation 300/2008**

Regulation (EC) No 300/2008<sup>55</sup> sets common rules in the field of aviation security, in order to protect civil aviation against acts of unlawful interference that jeopardise the security of civil aviation. The second objective of the Regulation is to provide the basis for a common, that is EU wide, interpretation of Annex 17 to the Chicago Convention. These two objectives are to be achieved by:

- (a) the setting of common rules and common basic standards on aviation security;
- (b) mechanisms for monitoring compliance.<sup>56</sup>

These common basic standards are laid down in the Annex to Regulation 300/2008.<sup>57</sup>

In line with Annex 17 – see Chapter 2.3 – Regulation 300/2008 provides for the setting up of national civil aviation security programmes and airport security programmes in the EU Member States. The national civil aviation security programmes “shall define responsibilities for the implementation of the common basic standards,” that are laid down in the Annex to this Regulation “and shall describe the measures required by operators and entities which it deems to have a legitimate interest.”<sup>58</sup> The airport security programmes “shall describe the methods and procedures which are to be followed by the airport operator in in order to comply both with this Regulation and with the national civil aviation security programme of the Member State in which the airport is located.”<sup>59</sup>

According to Article 14 of Regulation 300/2008, under a national civil aviation security programme entities may be required to set up a security programme of their own. Such a programme “shall describe the methods and procedures which are to be followed by the entity in order to comply with the national civil aviation security programme of the Member State in respect of its operations in that Member State.”<sup>60</sup>

---

<sup>55</sup> Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, OJ L 97, 9.4.2008

<sup>56</sup> *Id.*, Article 1

<sup>57</sup> *Id.*, Article 4

<sup>58</sup> *Id.*, Article 10

<sup>59</sup> *Id.*, Article 12

<sup>60</sup> *Id.*, Article 14

The Annex to Regulation 300/2008 does not so much refer to aspects clearly falling within the scope of an RTP, but merely addresses more general security aspects, relating to airport planning requirements, access control, surveillance and patrols, screening of passengers and baggage, and security control for cargo and mail.

So for the scope of this thesis, the relevance of this Regulation lays in the fact that it points out that under this Regulation, RTPs are not considered in relation to aviation security and that therefore RTPs as such do not affect the regulations on aviation security.

### **3.2.2 Regulation 18/2010**

Commission Regulation (EU) No 18/2010<sup>61</sup> [hereafter: Regulation 18/2010] provides an Annex with specifications for national quality control programmes in the field of civil aviation security. The objectives of the national quality control programme consist in verifying “aviation security measures to be effectively and properly implemented” and determining “the level of compliance with the provisions of this Regulation and the national civil aviation security programme.”<sup>62</sup> However, as long as RTPs do not fall within the scope of civil aviation security programmes, they are not affected by Regulation 18/2010.

### **3.3 Regulation 185/2010, as amended by Regulation 173/2012**

Commission Regulation (EU) No 185/2010<sup>63</sup> lays down measures for the implementation of common basic standards on aviation security.<sup>64</sup> Since its entry into force, it has been amended twice: first by Regulation 173/2012 and recently by Regulation 654/2013. However, Regulation 654/2013,<sup>65</sup> applying to mail and cargo, falls outside the scope of this thesis.

---

<sup>61</sup> Commission Regulation (EU) No 18/2010 of 8 January 2010 amending Regulation (EC) No 300/2008 of the European Parliament and of the Council as far as specifications for national quality control programmes in the field of civil aviation security are concerned, OJ L 7, 12.1.2010

<sup>62</sup> *Id.*, Annex (3.1)

<sup>63</sup> Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security, OJ L 55, 5.3.2010

<sup>64</sup> *Id.*, Article 1: “This Regulation lays down detailed measures for the implementation of common basic standards for safeguarding civil aviation against acts of unlawful interference that jeopardise the security of civil aviation and general measures supplementing the common basic standards. “

<sup>65</sup> Commission Implementing Regulation (EU) No 654/2013 of 10 July 2013 amending Regulation (EU) 185/2010 in respect of EU aviation security validation checklists for third country entities, OJ L 190, 11.7.2013



### 3.3.1 Regulation 185/2010

The adoption of measures for the implementation of the common basic standards on aviation security is done in accordance with Article 4 of Regulation 300/2008.<sup>66</sup>

Some of these common basic standards may contain sensitive security measures, which then should be regarded as EU classified information and which therefore should not be made public. These measures are to be adopted separately, “by means of a Decision addressed to the Member States.”<sup>67</sup>

The non-classified measures implementing common basic standards are set out in the Annex to Regulation 185/2010, of which the provisions on security restricted areas and access to these areas are the most relevant for this thesis. Security restricted areas are defined as follows “a part of the airport to which screened departing passengers have access.”<sup>68</sup>

Access to security restricted areas is only allowed to persons that have a legitimate reason to be there. For being granted access to a security restricted area one way of authorisation is a valid boarding card or equivalent (Annex: 1.2.2.2). This boarding card or equivalent must be checked before a person is granted access, for the purpose of establishing its validity and correspondence with the holder’s identity (Annex: 1.2.2.4). For the prevention of unauthorised access to these areas, their entry points must be controlled by an electronic system, or by an authorised person assigned for this task.<sup>69</sup>

In other words, according to Regulation 185/2010 participation in an RTP does not grant a person access to security restricted areas, as an RTP smart card or token can in no way be regarded as a boarding pass or equivalent. Participation in an RTP does not have consequences for Regulation 185/2010.

### 3.3.2 Regulation 173/2012

Commission Implementing Regulation (EU) No 173/2012<sup>70</sup> amends Regulation 185/2010. It is relevant for this thesis with regards to the following amendments – which are listed in the Annex to Regulation 173/2012:

(2) the following paragraph is added to point 1.2.2.2:

‘Alternatively, access may also be granted after positive identification via biometric data verification.’;

(3) the following paragraph is added to point 1.2.2.4:

---

<sup>66</sup> *Supra*, note 63, Preamble (1)

<sup>67</sup> *Id.*, Preamble (2)

<sup>68</sup> *Id.*, Annex (1.1.2.1(a))

<sup>69</sup> *Id.*, Annex (1.2.2)

<sup>70</sup> Commission Implementing Regulation (EU) No 173/2012 of 29 February 2012 amending Regulation (EU) No 185/2010 as regards clarification and simplification of certain specific aviation security measures, OJ L 59, 1.3.2012

‘Where biometric identification is used, the verification shall ensure that the person seeking access to security restricted areas holds one of the authorisations listed under point 1.2.2.2 and that this authorisation is valid and was not disabled.’

This implies that, while being in a possession of a valid boarding card or equivalent is still mandatory, access can be granted by means of biometric identification, which may be biometric identification under an RTP. This provision needs adaptation: it can never have been the intention to let people pass by their biometric identification. A check for boarding card is still needed – the obligation to be in possession of such a valid boarding card alone does not suffice.

### **3.4 Regulation 1077/2011**

Regulation (EU) 1077/2011 establishes a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.<sup>71</sup> Its content is therefore rather operational of character, as will be demonstrated hereafter.

The Agency deals with SIS II (Schengen Information System: Article 3), VIS (the Visa Information System: Article 4), and Eurodac (a system concerning fingerprints: Article 5). Only if so provided by relevant legislative instruments, based on articles 67-89 TFEU, then the Agency “may also be made responsible for the preparation, development and operational management of large-scale IT systems in the area of freedom, security and justice” other than the three mentioned above.<sup>72</sup>

This means that if so provided for legally, the Agency may also be involved in the technical development, maintenance and control of an EU RTP. As we will see in chapter 5, this is indeed the case.

The Agency has the obligation to ensure an “effective, secure and continuous operation of large-scale IT systems” and “a high level of data protection, in accordance with the applicable rules, including specific provisions for each large-scale IT system”<sup>73</sup>

### **3.5 Conclusions Chapter 3**

Regulation (EC) No 562/2006 on the rules governing the movement of persons across the external borders of the Member States of the European Union can be taken up as an incentive for the adoption of an RTP, from a practical point of view mainly for two reasons: the application of an RTP would reduce border crossing time, reducing the need to relax checks at busy times; and secondly, by

---

<sup>71</sup> Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011

<sup>72</sup> *Supra*, note 71, Article 1(3)

<sup>73</sup> *Id.*, Article 2

use of an RTP, the ‘physical’ stamping can be replaced by ‘electronic stamping’, that is scanning of the RTP-token. Regulation (EC) No 562/2006 also provides for an overview of items that could be included in RTP’s central database and/or token, as well as the three different categories of stamps for documents which could be done electronically under an RTP – by scanning instead of stamping.

With regards to privacy and data protection reference is made to the Charter of Fundamental Rights of the European Union has been referred to as an extra safeguard and assurance that these are protected.

Regulation (EC) No 300/2008 firstly set common basic standards in the field of aviation security, and secondly provides the basis for an EU wide, uniform, interpretation of Annex 17 to the Chicago Convention. These common basic standards are laid down in the Annex to the Regulation, which, as said, addresses general security aspects, relating to airport planning requirements, access control, surveillance and patrols, screening of passengers and baggage, and security control for cargo and mail, and not so much aspects specifically relating to RTPs. Regulation 18/2010 specifies the requirements of national quality control programmes in the field of aviation security. The relevance of these two Regulations lays therefore in the fact that it shows that under these Regulations, RTPs are not considered in relation to aviation security and that therefore RTPs as such do not affect the regulations on aviation security.

Commission Regulation (EU) No 185/2010, amended by Regulation (EU) No 173/2012, lays down measures for the implementation of common basic standards on aviation security. The Regulation as amended foresees in access to security restricted areas by biometric identification. It seems that this provision is adopted without taking into account that that could imply that biometric identification alone suffices. For the sake of security this provisions should be adapted and specified, so to exclude persons with biometric identification without valid boarding cards or equivalent.

Finally, Regulation (EU) 1077/2011 addresses the establishment of a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. This Agency may, if so legally provided, be involved in the technicalities of a EU RTP.

## CHAPTER 4: EXISTING REGISTERED TRAVELLER PROGRAMMES IN THE NETHERLANDS AND THE UNITED STATES

### **4.1 The relevance of national law**

In the field of law relating to Registered Traveller Programmes, States are bound by international Law – and for the EU Member States, also by EU Law – as explained in Chapter 2 and 3 and for as far as this law is provided. Where legislation is needed with relation to RTPs and this is not provided by international law and/or EU law, States must enact their own domestic legislation. National laws on RTPs will therefore vary from State to State. In this chapter 4 I will discuss existing RTPs, in two States, that is the Netherlands and the United States.

### **4.2 The Netherlands**

The RTP in the Netherlands is called Privium<sup>74</sup> and runs at Amsterdam Airport Schiphol. Amsterdam Airport Schiphol itself is an independent and commercial entity. Its shares are in possession of the State of the Netherlands (70%), the municipality of Amsterdam (20%), Aéroports de Paris (8%), and the municipality of Rotterdam (2%).<sup>75</sup>

The biometrics applied for the Privium RTP is iris recognition. An iris pattern is unique for each individual. With the biometric data stored on a Privium card, the Privium member authenticates himself at the Privium gate. The software behind the iris scan has been developed by Schiphol, in collaboration with the Dutch Immigration and Naturalisation Service<sup>76</sup> (in Dutch: ‘IND’) and the Dutch Military Police, also called Royal Netherlands Marechaussee<sup>77</sup> (in Dutch: ‘Koninklijke Marechaussee’). Schiphol is the owner of the equipment and software.

When a person applies for Privium membership and gets approved, he enters into a contractual relationship with Schiphol.<sup>78</sup> Upon issuance of the Privium card the member’s passport is being checked by the Royal Netherlands Marechaussee. Also the person is being interviewed as part of the verification that the person is of irreproachable conduct and does not constitute a security threat in any way. On the Privium card there is the card number, the template of the iris scan, the name and the date of birth of the participant, “as well as data derived from them that are required for providing Privium Services” (Article 7.2 of the Terms and Conditions). Interestingly, according to the Terms

---

<sup>74</sup> ([www.schiphol.nl/Travellers/AtSchiphol/Privium.htm](http://www.schiphol.nl/Travellers/AtSchiphol/Privium.htm)), last visited (14 July 2013)

<sup>75</sup> ([www.jaarverslagschiphol.nl/over-ons/profiel](http://www.jaarverslagschiphol.nl/over-ons/profiel)), last visited (14 July 2013)

<sup>76</sup> (<http://www.ind.nl/EN/Pages/default.aspx>), last visited (14 July 2013)

<sup>77</sup> (<http://www.defensie.nl/english/marechaussee>), last visited (14 July 2013)

<sup>78</sup> See for the Privium terms and conditions in English:

([www.schiphol.nl/Travellers/AtSchiphol/Privium/Privium/Membership/Membership/RegisterPriviumMembership.htm](http://www.schiphol.nl/Travellers/AtSchiphol/Privium/Privium/Membership/Membership/RegisterPriviumMembership.htm)), last visited (14 July 2013)

and Conditions also the place of birth is contained on the Privium card. However, in practice it appears that there is no place of birth on the Privium card. So if it is there, it must be stored on the chip in the card.

Subsequently, at each border crossing the police registers are checked automatically – instead of requested by hand. So the passport control remains in the hands of a government service, but is done in an automated way. Verification of the identity of the person is done by iris recognition. The biometric information is stored on the Privium card that is held by the Privium member. There is no central database where these biometric data are stored!<sup>79</sup> Schiphol is officially the owner of the Privium card. For the provision of the Privium card, Schiphol charges a fee. There are three types of membership: Basic, for EUR 121 per year; Privium Plus, for EUR 199 per year; and a Partner Card for EUR 73 per year.<sup>80</sup> The Privium Plus membership offers extra, such as priority parking, access to the Privium Club Lounge, business class check-in with participating airlines, e-newsletter Privium update, discounts on Schiphol Excellence Parking, discounts on Schiphol Valet Parking and discounts at Schiphol Plaza.<sup>81</sup> It follows that apart from a regulation on fast border crossing, Privium is also used as a commercial tool.

Privium membership is open to citizens of the EU Member States and, Iceland, Liechtenstein, Norway and Switzerland. For all other citizens it is only possible to become a member of Privium when they hold a specific diplomatic identity card issued by the Dutch Ministry of Foreign Affairs.<sup>82</sup>

According to Article 7.1 of the Terms and Conditions of Privium Membership, the personal data that are collected by Schiphol are the ones that the Privium applicant has provided on the application form, as well as the data on the use of the Privium card. Schiphol states that it complies with the statutory regulations as laid down in the Dutch Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*), which is the act implementing Directive 95/46/EC, as to which see Chapter 6.4.

In Article 7.3 Schiphol promises to prevent unauthorized use of Privium cards. Schiphol has entered into data processor agreements with third parties to which services are outsourced.

Within the scope of Privium, the following personal data are processed (Article 7.4):

the date and time at which the Privium Card is inserted into the card reader of the Automatic Border Passage. Within the scope of the Automatic Border Passage, the

---

<sup>79</sup> Information provided in an email dating 28 June 2013 by Schiphol to the author

<sup>80</sup> (<http://www.schiphol.nl/Travellers/AtSchiphol/Privium/Privium/Membership.htm>), last visited (14 July 2013)

<sup>81</sup> *Id.*

<sup>82</sup> *Supra*, note 78

Dutch Military Police (Koninklijke Marechaussee) shall be provided with the personal data required for the performance of its duties.

Furthermore according to Article 7.7, Schiphol does not share the Participant's personal data with others outside the Schiphol Group, with permission from the Privium Member, *except* "where this is required by law and in cases referred in the Privium Participation Agreement," that is to the Dutch Military Police.

In its Terms and Conditions, Schiphol also provides that the Privium Member can request his data that are collected by Schiphol (Article 7.8).

Through Article 8.1 Schiphol limits its liability for damage connected with the Privium card and/or Privium services to the annual subscription fee. However, this limit does not apply "if and insofar as Schiphol can be sued on the basis of mandatory applicable law (e.g. product liability law), as well as in the event of willful intent or gross negligence on the part of Schiphol or its executive staff."

### **4.3 United States**

#### **4.3.1 Registered Traveller Programmes in the U.S.**

In the U.S. there are two RTPs in international civil aviation: Global Entry and NEXUS.<sup>83</sup>

Global Entry is a government driven RTP,<sup>84</sup> executed under the flag of the U.S. Customs and Border Protection [hereafter: CBP]. Participants need to be pre-approved, by means of a background check and an interview.<sup>85</sup> The Global Entry RTP kiosks are available at thirty-one airports in the US, eight airports in Canada, two airports in Ireland, and the airports of San Jose in Puerto Rico, Guam and the Northern Mariana Islands.<sup>86</sup> Membership of Global Entry is open to U.S. citizens, U.S. lawful permanent residents, as well as Dutch citizens that are enrolled in Privium, Korean citizens enrolled in Smart Entry Service – the South-Korean RTP – and Mexican citizens. Canadian citizens enrolled in the NEXUS RTP have Global Entry benefits, but cannot join.<sup>87</sup>

Participants need to make sure via an online system that they keep their personal details up-to-date.

Apart from use at airports Global Entry is also used for land sea border crossings. For crossing borders at airports, no separate card are issued; Members pass the borders at the kiosk using their passport or lawful permanent resident card. The biometrics used are fingerprints.<sup>88</sup>

---

<sup>83</sup> ([www.cbp.gov/xp/cgov/travel/trusted\\_traveler/](http://www.cbp.gov/xp/cgov/travel/trusted_traveler/)), last visited (15 July 2013)

<sup>84</sup> ([www.globalentry.gov](http://www.globalentry.gov)), last visited (15 July 2013)

<sup>85</sup> ([www.globalentry.gov/about.html](http://www.globalentry.gov/about.html)), last visited (15 July 2013)

<sup>86</sup> ([www.globalentry.gov/locations.html](http://www.globalentry.gov/locations.html)), last visited (15 July 2013)

<sup>87</sup> ([www.globalentry.gov/faq.html](http://www.globalentry.gov/faq.html)), last visited (15 July 2013)

<sup>88</sup> *Supra*, note 78

The Terms and Conditions are not publicly available online; in order to have access you have to apply for the programme first.

If an applicant has ever been convicted of any criminal offense, or when he has pending criminal charges, his application will be refused.<sup>89</sup>

The NEXUS programme, which uses iris recognition as its biometric,<sup>90</sup> exists next to the Global Entry programme, and is interoperable with it. NEXUS is specifically designed for border traffic between the United States and Canada, and applies to air, land and sea traffic.<sup>91</sup>

#### **4.3.2 Registered Traveller Programmes under U.S. Law**

With regards to U.S. Law, the following legislation is relevant:

- Privacy Act (1974), as amended
- Aviation and Transportation Security Act (2001)
- Intelligence Reform and Terrorism Prevention Act (2004)
- Department of Homeland Security Appropriations Act (2006)
- Consolidated Appropriations Act (2008)

The Aviation and Transport Security Act of 2001<sup>92</sup> and the Intelligence Reform and Terrorism Prevention Act of 2004<sup>93</sup> form the legal basis for the establishment of RTPs in the United States. Already under the Aviation and Transport Security Act it was decided that requirements should be established to enable the implementation of ‘trusted traveler programs’ and “use available technologies to expedite the security screening of passengers who participate in such programme, thereby allowing security screening personnel to focus on those passengers who should be subject to more extensive screening.”<sup>94</sup> Besides the biometric entry and exit system that was set up for international travellers entering the United States. Under Sec. 7208(k)(3)(A) of the Intelligence Reform and Terrorism Prevention Act, it is provided that “as soon as is practicable, the Secretary shall develop and implement a registered traveler program to expedite the processing of registered travelers who enter and exit the United States.” Under Sec. 7208(k)(2) ‘registered traveler program’ has been defined as “any program designed to expedite the travel of previously screened and known travelers across the borders of the United States.” Furthermore it was stated that:

---

<sup>89</sup> *Supra*, note 78

<sup>90</sup> ([usa.immigrationvisaforms.com/travel/nexus-iris-scan-locations](http://usa.immigrationvisaforms.com/travel/nexus-iris-scan-locations)), last visited (16 July 2013)

<sup>91</sup> ([www.cbp.gov/xp/cgov/travel/trusted\\_traveler/nexus\\_prog/](http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/)), last visited (15 July 2013)

<sup>92</sup> Aviation and Transportation Security Act, Pub. L. 107-71, title I, Sec 109, Nov. 19, 2001, as amended by Pub. L. 107-296, title XIV, Sec. 1403(b), Nov. 25, 2002

<sup>93</sup> Intelligence Reform and Terrorism Prevention Act, Pub. L. 108-458, 6. U.S.C. 485, Dec. 17, 2004

<sup>94</sup> *Supra*, note 92

The registered traveler program shall include as many participants as practicable by

- (i) minimizing the cost of enrolment;
- (ii) making program enrollment convenient and easily accessible; and
- (iii) providing applicants with clear and consistent eligibility guidelines.<sup>95</sup>

The RTP in the U.S. is clearly government-driven without any commercial aims and is once again motivated under Sec. 7208(k)(1)(B):

The process of expediting travelers across the borders of the United States can permit inspectors to better focus on identifying terrorists attempting to enter the United States.

As will be shown in Chapter 5, the same line of reasoning is followed in the EU Proposal for a Regulation establishing an RTP.

The 2008 Consolidated Appropriations Act<sup>96</sup> specifies the use of a biometrically-secure Registered Traveler card: approved members of an RTP may fully satisfy the required identity verification procedures at security screening checkpoints by presenting this card instead of the government-issued photo identification document required of non-participants.

The topic of enrolment cost referred to in the Intelligence Reform and Terrorism Prevention Act of 2004 is elaborated upon in the 2006 Department of Homeland Security Appropriations Act,<sup>97</sup> which provides that the fee is set by the Department of Homeland Security and that it may not exceed total aggregate costs of the RTP.

The last act to discuss is the Privacy Act of 1974, as amended.<sup>98</sup> By rule of the Transportation Security Administration [hereafter: TSA], since July 8, 2005, Registered Traveler Operations Files are exempted from a number of the provisions of the Privacy act of 1974 in order for the security aspects to function properly, and to prevent the unauthorised disclosure of classified and law enforcement information.<sup>99</sup> These provisions are:

(c)(3) – accounting of disclosures; (d) – access to records; (e)(1) – relevancy and necessity of information; (e)(4)(G), (H), and (I) – agency requirements; and (f) – agency rules. The exemptions are

---

<sup>95</sup> *Supra*, note 93

<sup>96</sup> Consolidated Appropriations Acts, Pub. L. 110-161, div. E, title V, Sec 571, Dec. 26, 2007

<sup>97</sup> Department of Homeland Security Appropriations Act, Pub. L. 109-90, title V, Sec. 540, Oct. 18, 2005

<sup>98</sup> Privacy Act of 1974, 5 U.S.C. § 552a

<sup>99</sup> Department of Homeland Security, Transportation Security Administration, 49 CFR Part 1507, [Docket No. TSA-2004-18984, Amendment 1507-1], RIN 1652-AA36, Federal Register, Vol. 70, No. 109, June 8, 2005



provided for by (k)(1) and (k)(2) of the Act. This means that the Agency controlling and processing personal data:

- does not have to provide to the individual, the date, nature and purpose of each disclosure of the record of that individual, and also the name and address of the person or agency to whom the disclosure has been made does not need to be revealed to the concerning individual (c)(3);
- does not have to permit an individual access to his record or any information pertaining to him and stored in the system, nor to permit the individual to request amendment of his record (d);
- does not have to maintain information in its records about an individual that is only relevant and necessary for achieving its purpose (e)(1);
- does not have to provide, when publishing in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, on said notice, the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him, nor on how he can get access to this record or contest it, nor the categories of sources of records in the system (e)(4)(G), (H), and (I); and
- does not have to provide procedures with regards to the individual and access to his record (f).<sup>100 101</sup>

#### **4.4 Conclusions Chapter 4**

While in practice providing to the same service to their participants, the backgrounds of the RTPs in the Netherlands and the United States are completely different: in the Netherlands, the programme originally seems to be commercially driven, with different service levels for different subscriptions for different fees. Biometric data are not stored centrally, but only on the smart card that is being carried by the RTP participant. Privacy and data protection wise Schiphol declares to apply the law, implementing EC directive 95/46 which restricts the use of and access to data, therewith protecting the interests of the individual.

How different is the situation in the United States, where the RTPs are government driven. The U.S. legislation providing for the establishment of RTPs clearly demonstrates that the point of departure in the United States - no pun intended – has been improving and speeding up the border control process in combination with safeguarding security. This is the main goal of the programme. It is provided explicitly that privacy and data protection restrictions do not apply to personal data provided by a person under an RTP.

---

<sup>100</sup> *Supra*, note 99

<sup>101</sup> *Supra*, note 98

## CHAPTER 5: THE PROPOSAL FOR AN RTP REGULATION IN THE EUROPEAN UNION

### **5.1 Proposal for a Regulation establishing a Registered Traveller Programme**

In February 2013, the European Commission introduced its Proposals for a Regulations on the establishment of an RTP.<sup>102</sup> In this chapter I will highlight the objectives, characteristics and legal elements of the proposal for a Regulation on the establishment of a Registered Traveller Programme.

#### **5.1.1 Objectives**

The objectives of this Proposal for a Regulation establishing an RTP, which is meant to be the “core instrument for the legal framework” of a European RTP, are threefold:

- to establish the procedures and conditions for access to the RTP;
- to define the purpose, the functionalities and responsibilities for a token-Central Repository as a system for the storage of data on registered travelers;
- to confer on the Agency for the operational management of large-scale information systems in the area of freedom, security and justice (the Agency), the development and operational management of the Central Repository and the definition of technical specifications for a token.<sup>103</sup>

#### **5.1.2 Characteristics**

The proposed RTP contains the following elements:

- the biometric data used are fingerprints;
- data are stored centrally in a Central Repository, under the auspices of the Agency;
- The RTP participant will be issued a token, in the form of a machine-readable card, containing only a unique identifier, that is an application number;
- In order to pass a border gate, the RTP participant will have to swipe the card, Then the gate will read the card, travel document and fingerprints, which will be compared to the data stored in the Central Repository – and other databases such as the Visa Information system [hereafter: VIS] for visa holders.<sup>104</sup>

Under the proposed EES entries and exits of third-country nationals will be registered, which is necessary for enabling full automation of border checks for RTP participants. It will also abolish the

---

<sup>102</sup> Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, COM(2013) 97 final, Brussels, 28.2.2013

<sup>103</sup> *Id.*, p. 4

<sup>104</sup> *Id.*, p. 3; article 3

obligation to stamp the passport,<sup>105</sup> which, as we have seen in chapter 3.1 is an obligation under Regulation 562/2006.

Whereas, the RTPs in the Netherlands and the US are primarily aimed at citizens of these States, as well as other EU/EEA States in the case of the Netherlands, or certain other States in the case of the U.S., the proposed EU RTP is aimed *solely* at third-country travellers who want to cross the external borders of the EU.

As in the U.S., the proposed RTP is government-driven and aims at speeding up the border process for registered travellers, therefore enabling border control to focus on the persons wanting to cross the border who are not participating in the RTP.

Lastly, the proposed RTP does not apply exclusively to border crossings via travelling by air, but applies to all Schengen border crossings!

### **5.1.3 Legal Elements**

The legal elements of the Proposed Regulation consist in short of the following:

- 1) definition of the purpose and functionalities of the RTP and accompanying token-Central Repository;
- 2) responsibilities for the RTP and token-Central Repository;
- 3) mandate for the Agency for the operational management of large-scale IT systems in the area of freedom, security and justice to develop, establish and operationally manage the central Repository;
- 4) procedures and conditions for the examination of an RTP application;
- 5) procedures and conditions for and the storage of data on registered travellers;
- 6) impact on fundamental rights, more specifically with regards to the protection of personal data (Article 8 of the Charter of Fundamental Rights of the EU) and the right to an effective remedy (Article 47 of the Charter).<sup>106</sup>

The proposal is very complete in all the different aspects it entails: procedures, technicalities, rights and obligations, liability, responsibilities, remedies: it is all provided for in the proposal.

## **5.2 Conclusions Chapter 5**

The EU Registered Traveller Programme, as set forth in the proposal, combines elements of both the RTP in the Netherlands and the RTPs in the United States, while at the same time having its own peculiarities. To start with the latter, most striking is that the EU RTP is aimed at frequent third country travellers, whereas the Dutch and U.S. RTPs originally aimed at nationals of these two States – in the case of the Netherlands extended with the availability for EU/EEA citizens as well.

---

<sup>105</sup> *Supra*, note 102, p. 3

<sup>106</sup> *Id.*, p. 7-8

Characteristics in common with the United States RTP are that the EU RTP is also government-driven and that it has a central database. In common with the Dutch RTP are the restrictions on the use of, access to and sharing of personal data. As said before under 5.1.3 of this chapter the proposed RTP Regulation is quite all-encompassing in the aspects it covers: competences, rights and obligations as well as responsibilities of the different parties involved have been addressed.

## CHAPTER 6: LEGAL ISSUES OF REGISTERED TRAVELLER PROGRAMMES

As demonstrated in the foregoing chapters, there is no legislation as such hindering the adoption of Registered Traveller Programmes, but that does not mean that there are no aspects not take into account. The aspects I have distilled are 1) aviation security standards, 2) the status of the RTP smart card or token as a travel document, 3) issues of liability, 4) privacy issues, and 5) data protection.

In this chapter I will further go into these issues.

### **6.1 Aviation security standards**

With regards to security standards, with the adoption of an RTP a State has to ensure that the quality of border control is not compromised. Under the Chicago Convention and its Annexes, guidelines are provided which States have given form as laws under domestic law, in order to comply with the provisions provided by the Chicago Convention and its Annexes. Under domestic law – and for the Netherlands also under EU law – the Netherlands and the United States have implemented their RTPs, and specified the tasks and responsibilities of the involved parties, such as the border control services and the airport. The same goes for the EU in its proposal for a Regulation establishing an RTP.<sup>107</sup>

Emphasized should be here that in the United States and the European Union the RTPs are government-driven, indeed with the intention to strengthen the safeguarding of security, with the underlying idea that the implementation of an RTP enables the border control services to focus on those persons who need the most attention, while spending much less time on the persons that are considered harmless.

So with relation to aviation security standards, the legal issue is that there are international treaty provisions by which 191 State are bound worldwide, as well as international standards an security that are applied globally. None of these may be infringed by the adoption of an RTP.

### **6.2 The status of the RTP smart card or token**

The status of the RTP smart card or token is not always that clear. Sometimes it seems that these are defined as travel documents, and other times it seems to be the opposite.

Whereas ICAO has developed standards for eVisas and ePassports, they have not done so for documents issued under an RTP, which seems to imply that from ICAO's point of view, an RTP document has not the same status. However, the same ICAO in its Annex 9 2005 edition has defined a travel document as “a passport or other official document of identity issued by a State or organization, which may be used by the rightful holder for international travel.” At that time the

---

<sup>107</sup> See also: Mendes de Leon, P., *The Fight against Terrorism through Aviation: Data Protection versus Data Production*, in: Air & Space Law, Vol. 31(4-5), 2006, p. 325

Privium RTP at Amsterdam Airport Schiphol was already running for some years. The following questions come to mind: is the Privium card an official document of identity? – There is not photo of the holder on it, but there are the biometric data of the holder, which makes him uniquely identifiable. What is “official”? Is Schiphol an “organization” as meant under this definition? Or is a private company not an organization? In the same Annex, ICAO provides the standard that a Contracting State “shall establish controls on the creation and issuance of travel documents.” Privium smart cards are issued by Schiphol, which is not a governmental body but a private company. Does that mean that the smart card is not a travel document? Or does the cooperation with the Dutch Military Police satisfy the condition of establishing controls? It is my impression that it has never been the intention to regard a RTP smart card or token as an official travel document of that same status as a passport. My argument for this is that since there are no international standards, it could lead to an unchecked proliferation of all sorts of ‘travel documents’, which is undesirable. In my view however the above questions should still be answered unambiguously in order to avoid confusion and uncertainty.

### **6.3 Issues of liability**

A liability issue could arise when a technical flaw in the automated process would not permit a harmless passenger to enter or depart a country.<sup>108</sup> Currently, border control ‘by hand’ by a customs officer is always available, and thus always should be, in order to enable border crossings, but what if due to all the hassle and loss of time in a case described above a passenger misses his flight?

The most logical would seem for the passenger to bring a claim against the RTP operator.

In the case of Privium in the Netherlands that would mean that the passenger could request compensation from Schiphol, that as mentioned in chapter 4, limits its liability for damage connected with the Privium card and/or Privium services to the annual subscription fee. However, this limit does not apply “if and insofar as Schiphol can be sued on the basis of mandatory applicable law (e.g. product liability law), as well as in the event of willful intent or gross negligence on the part of Schiphol or its executive staff” (Article 8.1 of the terms and conditions). In the case of the EU proposal the liability lies with the Member States.

### **6.4 Privacy rights and data protection**

First of all I want to point out that participation in a RTP is on a voluntary basis. If someone joins an RTP, he enters into an agreement with the RTP operator. The RTP operator must provide information how it is going to use the personal data of the applicant, and if they are going to be used

---

<sup>108</sup> Abeyratne, R., *The Automated Screening of Passengers and the Smart Card – Emerging Legal Issues*, in: *Air & Space Law*, Vol. 23(1), 1998, p. 4

for other purposes than the RTP itself, and if the personal data are going to be shared with other parties.

Ruwantissa Abeyratne in his book *Aviation Security Law* distinguishes between three rights of privacy relating to the storage and use of personal data:

- 1) The right of an individual to determine what information about oneself to share with others, and to control the disclosure of personal data.
- 2) The right of an individual to know what data is disclosed, and what data is collected and where such is stored when the data in question pertains to that individual; the right to dispute incomplete or inaccurate data.
- 3) The right of people who have a legitimate right to know in order to maintain the health and safety of society and to monitor and evaluate the activities of government.<sup>109</sup>

In other words, these rights represent a balance of rights: on the one hand the right of the individual to determine the sharing and disclosure of his own personal data, and on the other hand the right of “a society to collect data about individuals that belong to it so that the orderly running of government is ensured.”<sup>110</sup>

These rights are also reflected in Directive 95/46/EC, which in the Netherlands is implemented under the Dutch law on Protection of Personal Data.

Directive 95/46/EC<sup>111</sup> obliges Member States to “protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.”<sup>112</sup> The Directive applies to the partly or wholly automated processing of personal data, however it does not apply to activities falling outside the scope of European Union law, such as those provided for by the at the time Titles V and VI of the Treaty on Provisions on a common foreign and security policy and Provisions on police and judicial cooperation in criminal matters, and in any case “to processing operations concerning public security, defence, State security (...) and the activities of the State in areas of criminal law.”<sup>113</sup>

The question now is – does that mean that also RTPs – which people join voluntarily – are excluded?

---

<sup>109</sup> Abeyratne, R., *Aviation Security Law*, Springer 2010, p. 59

<sup>110</sup> *Id.*

<sup>111</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.95

<sup>112</sup> *Id.*, Article 1

<sup>113</sup> *Id.*, Article 3

My first response would be yes: RTPs provide for an automated system of border control, which in my view must be regarded as a 'processing operation concerning public security' as provided for in Article 3 of Directive 95/46. This can also be upheld in the light that the RTPs in the United States and in the EU proposal are governmental driven programmes. In the Netherlands however, under the Privium RTP, participants have entered into an agreement with a private party, that is Schiphol.

As said, Directive 95/46/EC has been implemented in the Netherlands through the Personal Data Protection Act, or in Dutch: *Wet Bescherming Persoonsgegevens*.<sup>114</sup> To answer the question whether or not RTPs fall within the scope of the Directive we go back to the Terms of Conditions of Privium where we read that Schiphol at least considers itself to be bound by the Personal Data Protection Act, implementing Directive 95/46/EC, and provides in its terms and conditions the restrictions and obligation resulting from the Directive, therewith implying the application of Directive 95/46/EC to at least the Privium RTP.<sup>115</sup>

As we have seen in chapter 4.3.2, the foregoing is in sheer contrast with the United States, where the data subject has less rights and the data controller less obligations, as demonstrated in said chapter.

A reason for this may well be that the U.S. regulations as indicated in chapter 4.3.2 apply specifically to Registered Traveller Programmes, being executed and set-up by governmental organs whereas Directive 95/46/EC is more general of character and also applies to private bodies.

## **6.5 Conclusions Chapter 6**

The legal issues I have discussed in this chapter show that the Regulation of RTPs involves a myriad of different topics. Some legal issues do not constitute necessarily a problem, but represent a serious matter not to be overlooked, such as aviation security and liability.

A second category exists of topics that could use some clarification, such as the status of the RTP smart card or token, and the distinction between the use of data under an RTP vs. the topic of PNR.

Lastly, with regards to privacy and data protection, we see that different RTPs provide for different regimes in this respect. In this thesis this has been demonstrated by the example of the Netherlands and the EU on the one hand, and the United States on the other hand. This might be something RTP participants may want to take into account when joining an RTP of a different State – when this option is available: by doing so, the same data may become subject to a complete other set of rules in terms of privacy and data protection.

---

<sup>114</sup> Wet Bescherming Persoonsgegevens, of 6 July 2000

<sup>115</sup> See chapter 4.2



## CONCLUSIONS AND RECOMMENDATIONS

The introduction and implementation of Registered Traveller Programmes is a rather recent development. By joining an RTP, the pre-vetted participants have the advantage of fast border crossing. The advantage for the RTP operator lays 1) in the fact that it enables border control to focus on the potentially more risky persons crossing the border, and 2) in the potential commercial benefits.

Even though it is not very likely that at the time of drafting the possibilities of RTPs were taken into account, the 1944 Chicago Convention contains a number of Articles that also apply to RTPs. While being rather general in scope, these Articles do not so much constitute an impediment for the establishment of RTPs, but provide for a number of conditions to be taken into account for the implementation of an RTP. The same goes for the discussed ICAO Annexes. In none of them is there any explicit mentioning of a Registered Traveller Programme, while at the time the phenomenon did already exist. It seems therefore that an RTP as such has not been considered an issue needing specific attention in relation to aviation security or airport operations and facilities. However, the way an RTP smart card or token has been defined could use some clarification. Even though in my opinion it would be undesirable to regard such an item as an official travel document, there are currently too many loopholes leaving room for this interpretation.

It is therefore worthwhile that this ambiguity would be addressed and clarified, preferably by ICAO as it has worldwide authority.

The relevant EU Regulations discussed are Regulation (EC) No 562/2006 on the rules governing the movement of persons across the external borders of the Member States of the European Union; Regulation (EC) No 300/2008 on common basic standards in the field of aviation security, as amended by Regulation 18/2010 ; Regulation (EU) No 185/2010, as amended by Regulation (EU) No 173/2012, laying down measures for the implementation of common basic standards on aviation security; and Regulation (EU) 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. Each of them is of specific relevance for the EU RTP as set forth in the 2013 proposal for an RTP Regulation.

Regulation (EC) No 562/2006 in my view can be considered as an incentive for the establishment of an RTP for the following two reasons: the application of an RTP would reduce border crossing time, reducing the need to relax checks at busy times; and secondly, by use of an RTP, the 'physical' stamping can be replaced by 'electronic stamping', that is scanning of the RTP-token.

Regulation (EC) No 300/2008 as amended by Regulation 18/2010 shows that in the specification of common basic standards on aviation security RTPs are not referred to and that therefore the adoption of an RTP does not have to affect aviation security regulations in the EU.

Regulation (EU) No 185/2010, as amended by Regulation (EU) No 173/2012, shows however that here the wording of the provisions on access to security restricted areas could need some fine-tuning for the sake of security. It seems that the addressed provision has been drawn up without taking into account the possible use and status of an RTP smart card or token.

Finally, Regulation (EU) 1077/2011 on the establishment of a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice provides for a practical requirement related to the technicalities of an RTP for the setting up of a European RTP.

So in general the existing relevant EU legislation provides an encouragement for an RTP in the EU, while at the same time only a minor adjustment need to be made as indicated above.

Looking at the existing RTPs in the Netherlands and the United States, I have put forward some remarkable characteristics that are not that obvious when you only look at the international and European legal framework. The RTP in the Netherlands is commercially driven, the one in the U.S. is government driven. In the Netherlands strict European regulations with respect to privacy and data protection apply, while in the U.S. these restrictions are mostly absent. The proposed EU RTP combines aspects of both: it involves a central database, as in the U.S., but applies restrictions on the use of and access to personal data and provides individuals with rights relating to the access and rectification of their personal data. Whatever option is preferred, I believe the most important is that the person joining an RTP is informed and knows what he agrees to when entering the programme.

In Chapter 6 I have addressed various legal aspects that need to be addressed when setting up an RTP. It shows that the range of topics is quite broad, and that the need for attention may vary from topic to topic. However as we live in a world where international civil air transport is expected only to grow, at least for the coming decades, I expect RTPs to be implemented more and more.

It would therefore be advisable in my view if ICAO would take up the topic and start working on standards for RTPs, especially in relation to airport operations and technical standards for RTP smart cards and tokens – which could also help to identify the legal status of this item – and in relation to aviation security, even if it were to confirm the *lack* of relation with aviation security.

## LIST OF SOURCES

### Treaties and related documents

- Chicago Convention on International Civil Aviation 1944, 15 UNTS 296-361 (1948)
- ICAO Annex 9 *Facilitation*, 12<sup>th</sup> ed., July 2005
- ICAO Annex 17 *Security*, 8<sup>th</sup> ed., April 2006

### European Union Law

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.95
- Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 105, 13.4.2006
- Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002, OJ L 97, 9.4.2008
- Commission Regulation (EU) No 18/2010 of 8 January 2010 amending Regulation (EC) No 300/2008 of the European Parliament and of the Council as far as specifications for national quality control programmes in the field of civil aviation security are concerned, OJ L 7, 12.1.2010
- Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security, OJ L 55, 5.3.2010
- Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ L 286, 1.11.2011
- Commission Implementing Regulation (EU) No 173/2012 of 29 February 2012 amending Regulation (EU) No 185/2010 as regards clarification and simplification of certain specific aviation security measures, OJ L 59, 1.3.2012
- Proposal for a Regulation of the European Parliament and of the Council establishing a Registered Traveller Programme, COM(2013) 97 final, Brussels, 28.2.2013
- Commission Implementing Regulation (EU) No 654/2013 of 10 July 2013 amending Regulation (EU) 185/2010 in respect of EU aviation security validation checklists for third country entities, OJ L 190, 11.7.2013

- Charter of Fundamental Rights of the European Union, OJ 2010 C83/02

#### **Dutch Law**

- Wet Bescherming Persoonsgegevens, July 6, 2000

#### **United States Law**

- Privacy Act of 1974, 5 U.S.C. § 552a
- Aviation and Transportation Security Act, Pub. L. 107-71, title I, Sec 109, Nov. 19, 2001, as amended by Pub. L. 107-296, title XIV, Sec. 1403(b), Nov. 25, 2002
- Intelligence Reform and Terrorism Prevention Act, Pub. L. 108-458, 6. U.S.C. 485, Dec. 17, 2004
- Department of Homeland Security Appropriations Act, Pub. L. 109-90, title V, Sec. 540, Oct. 18, 2005
- Consolidated Appropriations Acts, Pub. L. 110-161, div. E, title V, Sec 571, Dec. 26, 2007
- Department of Homeland Security, Transportation Security Administration, 49 CFR Part 1507, [Docket No. TSA-2004-18984, Amendment 1507-1], RIN 1652-AA36, Federal Register, Vol. 70, No. 109, June 8, 2005

#### **ICAO Documents**

- ICAO Doc 7670 Resolutions and Recommendations of the Assembly 1st to 9th Sessions (1947-1955), Montreal, Canada, 1956
- Doc 9303 Machine Readable Travel Documents, Part 1, Vol. 1, 6<sup>th</sup> edition, 2006
- Doc 9303 Machine Readable Travel Documents, Part 1, Vol. 2, 6<sup>th</sup> edition, 2006
- Doc 9303 Machine Readable Travel Documents, Part 2, 3<sup>rd</sup> edition, 2005
- Doc 9303 Machine Readable Travel Documents, Part 3, Vol. 1, 3<sup>rd</sup> edition, 2008
- Doc 9303 Machine Readable Travel Documents, Part 3, Vol. 2, 3<sup>rd</sup> edition, 2008
- Supplement to Doc 9303, 4 April 2013
- Doc 9902 Assembly Resolutions in Force (as of 28 September 2007)

#### **ICAO Assembly resolutions**

- Resolution A1-31 Definition of International Standards and Recommended Practices
- Resolution A36-13 Consolidated Statement of ICAO policies and associated practices related specifically to air navigation

## Books

- Abeyratne, R., *Aviation Security Law*, Springer 2010
- Dr. Jiefang Huang, *Aviation Safety and ICAO* (Doctoral Thesis Leiden University), Kluwer Law International/E.M. Meijers Institute for Legal Research, 2009
- Milde, M., *International Air Law and ICAO (Essential Air and Space Law 4)*, Eleven International Publishing, 2008

## Articles

- Abeyratne, R., *The Automated Screening of Passengers and the Smart Card – Emerging Legal Issues*, in: *Air & Space Law*, Vol. 23(1), 1998, pp. 3-7
- Abeyratne, R., *Attacks on America – Privacy Implications of Heightened Security Measures in the United States, Europe, and Canada*, in: *Journal of Air Law and Commerce*, Vol. 67(1), 2002, pp. 83-115
- Hong, J., *Liability of Aviation Security Service Providers and Responsibility of States*, in: *Air & Space Law*, Vol. 35(1), 2010, pp. 9-32
- Lockie, M. (ed.), *Registered traveller update*, in: *Biometric Technology Today*, Vol. 15(6), 2007, pp. 9-12
- Lockie, M. (ed.), *RTPs keep the world moving*, in: *Biometric Technology Today*, Vol. 16(7-8), 2008, pp. 10-11
- Mendes de Leon, P., *The Fight against Terrorism through Aviation: Data Protection versus Data Production*, in: *Air & Space Law*, Vol. 31(4-5), 2006, pp. 320-330
- Piera, A., *The Simplifying Passenger Travel Programme and its Legal Implications*, in: *Air & Space Law*, Vol. 28(3), 2003, pp. 132-138

## Websites

- [usa.immigrationvisaforms.com/travel/nexus-iris-scan-locations](http://usa.immigrationvisaforms.com/travel/nexus-iris-scan-locations), last visited 16 July 2013
- [www.cbp.gov/xp/cgov/travel/trusted\\_traveler/](http://www.cbp.gov/xp/cgov/travel/trusted_traveler/), last visited 15 July 2013
- [www.cbp.gov/xp/cgov/travel/trusted\\_traveler/nexus\\_prog/](http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/), last visited 15 July 2013
- [www.defensie.nl/english/marechaussee](http://www.defensie.nl/english/marechaussee), last visited 14 July 2013
- [www.globalentry.gov](http://www.globalentry.gov), last visited 15 July 2013
- [www.globalentry.gov/about.html](http://www.globalentry.gov/about.html), last visited 15 July 2013
- [www.globalentry.gov/faq.html](http://www.globalentry.gov/faq.html), last visited 15 July 2013
- [www.globalentry.gov/locations.html](http://www.globalentry.gov/locations.html), last visited 15 July 2013
- [www.icao.int/secretariat/legal/List%20of%20Parties/Chicago\\_EN.pdf](http://www.icao.int/secretariat/legal/List%20of%20Parties/Chicago_EN.pdf), last visited 7 July 2013

- [www.ind.nl/EN/Pages/default.aspx](http://www.ind.nl/EN/Pages/default.aspx), last visited 14 July 2013
- [www.jaarverslagschiphol.nl/over-ons/profiel](http://www.jaarverslagschiphol.nl/over-ons/profiel), last visited 14 July 2013
- [www.schiphol.nl/Travellers/AtSchiphol/Privium.htm](http://www.schiphol.nl/Travellers/AtSchiphol/Privium.htm), last visited 14 July 2013
- [www.schiphol.nl/Travellers/AtSchiphol/Privium/Privium/Membership.htm](http://www.schiphol.nl/Travellers/AtSchiphol/Privium/Privium/Membership.htm), last visited 14 July 2013
- [www.schiphol.nl/Travellers/AtSchiphol/Privium/Privium/Membership/Membership/RegistrarPriviumMembership.htm](http://www.schiphol.nl/Travellers/AtSchiphol/Privium/Privium/Membership/Membership/RegistrarPriviumMembership.htm), last visited 14 July 2013

### **Other**

- Personal email from Schiphol to the author, dated 28 June 2013