SIAM

Security Impact Assessment Measures

WP 9

Legal Frameworks –

Regulative Techniques

Deliverable D9.8

Evaluation of case study reports

& further findings

Project Group Constitutionally Compatible Technology Design

Kassel University

Prof. Dr. Alexander Roßnagel

Christian Ludwig Geminn

Project number
261826

Call (part) identifier
FP7-Security-2010-1

Funding scheme
Collaborative Project

Table of Contents

Abbreviations

ACPO	Association of Chief Police Officers
Art.	Article
Az.	Aktenzeichen, file reference
BGBl.	Bundesgesetzblatt, official periodical of German Federal Law
BPolG	Bundespolizeigesetz / German Federal Police Act
BVerfG	Bundesverfassungsgericht / German Federal Constitutional Court
BVerfGE	Decision of the German Federal Constitutional Court
C	Consideration
CCTV	Closed-circuit Television
cf.	confer
CIT	Counter Infringement Technology
D	Deliverable
Doc	Document
EC	European Community
ECAC	European Civil Aviation Conference
Ed.	Editor(s)
EU	European Union
ECJ	European Court of Justice
f./ff.	following
FP	Framework Programme
ICAO	International Civil Aviation Organisation
ICTAF	Interdisciplinary Center for Technological Analysis and Forecasting
JurPC	Internet-Zeitschrift für Rechtsinformatik und Informationsrecht, journal
LAGs	Liquids, Aerosols and Gels
No	Numero
LuftSiG	Luftsicherheitsgesetz / German Aviation Security Act
OPS	Operations
OVG	Oberverwaltungsgericht, Higher Administrative Court (Germany)
para.	Paragraph
SIAM	Security Impact Assessment Measures
SiTI	Istituto Superiore sui Sistemi Territoriali per l'Innovazione
SMT	Security Measure and Technology
SWD	Commission Staff Working Document
TUB	Technische Universität Berlin
ZLW	Zeitschrift für Luft- und Weltraumrecht, journal
v.	von
Vol.	Volume

1. Introduction

This deliverable serves the following purposes:

- to provide a critical evaluation of the data gathered in deliverables 9.3, 9.4, 9.5 and 9.6 of the SIAM project. These deliverables have provided valuable insight into the legal framework of the use of SMTs at the four SIAM case study sites;
- to provide a critical assessment of legal regulation as a CIT and to give recommendations on how regulations can be configured for the proper implementation in order to ensure the protection of basic rights;
- to provide a comparison of the levels of freedom protection of those groups that are affected by SMTs that have been identified in work package 4;
- to demonstrate the implications of using unidirectional data management procedures in surveillance systems; and
- to provide input for the SIAM Assessment Support Tool.

Deliverable 9.8 concludes the research efforts in work package 9 of the SIAM project, whose aims were to find out whether implemented regulatory techniques achieve their objectives and are appropriate to the challenges of evolving, more intensive and extensive security technologies and practices, and to identify lacks of regulation; all the while building on the information gathered in all previous work packages of the SIAM project. Work package 9 was however most closely connected to work packages 2, 4, 5 and 8. Work packages 2 and 5 have provided information on present and future technologies and have given an indication for the challenges that the legal regulation of SMTs poses. Work package 4 has looked at different groups of actors that come in contact with SMTs. Work package 8 has amended this by providing insight into the types of freedom infringements passengers are subjected to when using mass transportation systems.

2. Evaluation of SIAM case study reports

The purpose of this chapter is to provide a critical evaluation and analysis of the data gathered in deliverables 9.3, 9.4, 9.5 and 9.6 of the SIAM project.

The primary methods of data acquisition were expert interviews and literature review. Interviewees were mainly legal experts and people involved in maintaining security at the case study sites.

2.1 Analysis of case study findings

Project partners TUB, SiTI and ICTAF were asked to provide a short literature review and to either perform interviews or a workshop with selected representatives from the case study sites as well as external experts with a profound knowledge of the legal framework of the use of SMTs at the case study sites.

To this end, the project partners were provided with a questionnaire that was to be administered to the selected experts. The full questionnaire consisted of a total of 28 sets of questions. It has been published in deliverable 9.1 of the SIAM project.

Responsibilities at case study sites

At the case study sites, the responsibility for the legal evaluation of SMTs usually lies with the security division, mostly in cooperation with the legal department. For instance, at Ben Gurion International Airport the legal departments of the Israel Airport Authority and the Israel Security Agency evaluate legal and ethical aspects of SMTs.

Oversight

All case study partners operate a security division which is responsible for the operation of SMTs. The case study partners themselves are overseen by public authorities that seek to ensure compliance with legal requirements. In civil aviation, additional oversight is provided by the International Civil Aviation Organisation which audits airports.

Compliance with legal requirements

The phenomenon that operators of public transport infrastructure comply merely with the minimum of what is legally required seems to be widespread. Interviewees from Italy cited ‘cultural factors’ when asked about the reasons for this. However, it seems that the phenomenon is far from being limited to Italy. This can be deducted from the attitude towards data protection that several interviewees expressed. Data protection seems to be considered a burden, a cost factor.

Additionally, adhering to the image of a necessary trade-off between liberty and security, legal requirements are often considered to hinder efforts to maintain

security. Following this logic, going beyond the legally mandated minimum when it comes to protect passenger rights will reduce security.

However, the main reason not to exceed minimum legal requirements is of an economic nature, since cost-effectiveness is one of the main principles of any business.

Influence of the law on SMT use and development

The interdependencies of law and technology have been discussed in depth in deliverable 9.2 of the SIAM project. The statements made during the interviews have confirmed the validity of what has been said in D9.2: Technology evolves at a rapid pace. The law must react in order to maintain its regency over the social cooperation amongst people. However, law makers rarely manage to anticipate technological developments and act pre-emptively. As a result, the law lags behind the constantly evolving technology in most cases.

When asked about the most influential laws on the use of SMTs, interviewees stated that in day-to-day operation privacy laws have the most profound effect.

Technological neutrality

When asked about their satisfaction with the clarity of the legal framework and its capability of covering future technologies, interviewees highlighted the concept of technological neutrality, which has already been discussed in chapter 2.1.2 of deliverable 9.2 of the SIAM project.

Legal requirements that are written in a technological neutral way, i.e. that apply to a wider range of technologies, secure the longevity of a norm. Technological neutrality means that a legal requirement can be applied to future technologies that were not envisioned when the requirement was enacted, thus increasing its transferability. This also means that where the concept of technological neutrality is used, there will rarely be any 'gaps' in regulations where a certain technology cannot be fitted into the legal framework.

Profiling

Profiling is considered an essential part of any security regime and thus its use is widespread. Still, the use of profiling is quite controversial, as it threatens a number of basic rights. As a result, the courts have reprimanded the way profiling is performed. Examples for this can be found in Israel (equality between Muslim and Jewish travelers) and in Germany (ban of profiling based on skin color). However, interviewees have argued that in Israel the order to cease the practice has had no effect on how profiling is performed in everyday operations at Ben Gurion airport.

Effectiveness of different regulative tools in preventing freedom infringements

When asked about the effectiveness of different regulative tools in preventing freedom infringements – not surprisingly – interviewees ranked voluntary agreements in which SMT operators pledge to bind themselves lowest and considered them ineffective. In return, the strongest regulative tools are those that are directly binding.

However, the effectiveness of any regulative tool is heavily linked with an effective oversight that ensures that any violations are detected and sanctioned.

The role of the courts

The courts may rule the use of certain SMTs illegal or demand changes to existing SMTs.

A very profound example for the role of the courts can be found in Israel. The concept of profiling as practiced in Israel meant a discrimination of Muslim travelers. A motion was made that demanded equality between Muslim and Jewish travelers. As a result, the attorney general instructed Ben Gurion International airport to provide for an equal treatment of travelers. In order to realize this, the system of luggage control was restructured. A test run of the new system began in June 2013. This illustrates the impact the courts can have on the use of an SMT as well as on a security regime as a whole.

Another example, which also deals with profiling, can be found in Germany. The Higher Administrative Court of Rheinland-Pfalz (OVG Rheinland-Pfalz)[1] ruled that id-checks by the German Federal Police, which is among other responsibilities charged with combatting illegal migration, are illegal if they are based on skin color.

Sanctions for violations of legal requirements

The interviewees named the following sanctions as possible options in case of a violation of legal requirements:

- fines,
- suspension/cessation of activities, and
- claims for compensation/damages.

Major differences between national legal requirements

When asked about major differences between national legal requirements that regulate the use of SMTs, the interviewed experts agreed that few differences remain within the European Union, particularly in the field of aviation security.

[1] OVG Rheinland-Pfalz, Decision of 29.10.2012, Az. 7 A 10532/12.OVG.

Some experts complained about low security standards in many countries outside the European Union, which hints at a lack of sufficient legal standards in these countries.

This question of national differences will be further investigated in chapter 3 of this deliverable, comparing the relevant legal framework in the Federal Republic of Germany and the United Kingdom as an example.

Problems arising from the diversity of national legal frameworks

Interviewees were asked how the security industry deals with the diversity of national legal frameworks. They expressed doubt whether SMT developers have a profound knowledge of national legal requirements. If this is indeed the case, it drastically reduces the influence of the law on the design and development process of SMTs: Those who are not aware of certain laws, cannot abide by them.

However, the diversity of national legal frameworks comes into play at the latest when marketing and selling a certain product in different countries. Thus, different national legal frameworks are a challenge that first and foremost big, internationally active companies have to face.

Harmonisation of legal requirements

Within the European Union, there seems to be a significant tendency towards legal harmonisation in the fields of data protection and aviation security. However, free space for the member states to implement their own policies remains. But the proposal for a General Data Protection Regulation, which is currently under debate, may diminish this free space when it comes to data protection.

On the international level, the Chicago Convention provides a basic level of harmonisation, which is however not as far-reaching as the harmonisation efforts within the European Union, which are in turn based on the Chicago Convention.[2] This harmonisation was triggered as early as 1944 and picked up even earlier efforts that date back to 1919. The reason behind this is the simple fact that civil aviation is an international phenomenon. Furthermore, civil aviation is and has been throughout the past century a booming industry and airplanes cross borders in next to no time. This made it necessary to develop and maintain a harmonised and coherent framework that secures a minimum standard.

Despite efforts to achieve some level of harmonisation in the areas of data protection and aviation security, policing and indeed the whole complex of laws relating to home affairs – being core aspects of the legitimation of any state – remain firmly under the control of the individual national states.

[2] See chapter 3 of this deliverable for a detailed description of the Chicago Convention.

Legal power to operate SMTs – Sweeping clauses vs. specific powers

When it comes to the legal basis for the operation of SMTs, there are two basic options for how to design a legal norm:

- A legal norm can include a sweeping clause that generally allows for the use of SMTs in a certain context, like security checks at airports.
- A legal norm can contain specific instructions which SMTs can be used, how they can be used and in what context they can be used.

A third option would be to not regulate the use of SMTs at all. This is however an option that entails significant threats to fundamental human rights. It is thus not a viable option. Where sweeping clauses exist (and even more so where no sub-constitutional regulation exists) constitutional law and the basic rights found within plays a central role as the key indicator which SMTs can be used and in what way. However, basic rights need to be concretised in order to extract specific requirements for the use of SMTs. Even where detailed legal requirements exist, it often becomes necessary to fall back on basic rights for guidance on how to configure a certain SMT. A detailed discussion of this issue can be found in deliverable 9.2 of the SIAM project, including a method for the concretisation of basic rights and the extraction of specific legal requirements from them.

Another way to indirectly influence the use of SMTs would be to use incentives like tax cuts or subsidies in order to promote certain SMTs and to make other SMTs less attractive.

Introducing new SMTs

The interviewees were asked, what usually sparks the introduction of new SMTs. Some of the keywords in their answers were ‘incident related’ and ‘driven by hysteria’. The introduction of new SMTs is highly incident related. Examples for this are the attempted terrorist attacks on 22 December 2001 (‘shoe bomber’), the Heathrow bomb plot of 2006 (‘liquid bomb plot’) and on 25 December 2009 (‘underwear bomber’) in the context of civil aviation. These terrorist activities resulted in X-ray controls of passengers’ shoes, restrictions on liquids in carry-on luggage and the advent of full body scanners. A specific incident leads to the introduction of a tailor-made security measure to combat this very scenario.

Similarly, terrorist incidents in the context of rail transport have resulted in debates on the expansion of surveillance systems in public transportation. It is thus generally acknowledged that the introduction of new SMTs in public transportation follows an action-reaction-scheme, which the interviewees affirmed and underlined with their answers.

Air Traffic vs. Rail Traffic

When comparing air traffic with rail traffic, security regimes at airports can be described as complex and highly regulated, while the opposite is true for rail traffic.

Security regimes at airports are fundamentally based on an international treaty, the Chicago Convention. In the European Union, the requirements of the Chicago Convention have been amended and concretized by the European Civil Aviation Conference Doc. 30 from which ultimately numerous regulations and directives are derived with even more detailed provision and legal requirements. The European regulations are then transformed into national law, which adds another layer of legal requirements and constraints. A detailed description of the legal framework can be found in chapter 3 of this deliverable. In simple terms, the law requires security checks of passengers, luggage and employees and contains rather specific details on how these checks can and cannot be conducted. Some interviewees thus characterised civil aviation security as 'over-regulated'.

Train security is predominately based on the use of CCTV, and while the use of surveillance cameras is highly regulated in most countries, there are no prescribed security measures that have to be implemented by law in order to maintain security.

In summary, the security regimes of civil aviation on the one hand and rail traffic on the other hand show fundamental differences. In civil aviation security, the main goal is to create 'safe zones' by installing security checkpoints which are designed to prevent the insertion of explosives, weapons and other hazardous articles into these zones, as well as to refuse access to all unauthorized persons. The main obstacle of any attacker is to overcome such a checkpoint. Ideally, the airside of an airport is such an airport in which exclusively such persons and objects are located that have undergone a stringent and thorough security check and that thus pose no risk to security. An airport is hence divided by a visible 'parting line'.

Such a line does not exist in rail traffic. While access to platforms is often limited to persons with valid tickets, even technical measures like turnstiles can only affirm that a person has gained the authority to enter by having purchased a valid ticket. Security measures that check for prohibited articles and create 'safe zones' similar to aviation security are not implemented. This is the result of the factual requirements of rail traffic: The rail infrastructure is too extensive and complex to allow for the creation of 'safe zones'; access has to be easy and quick, unhampered by extensive security checks. The challenges of maintaining a state of security in rail traffic are thus fundamentally different than in air traffic which is mirrored by the relevant legal framework.

Cultural differences

A key factor is the perceived importance of privacy versus security. Cultural imprints lead to different priorities which are mirrored in the legal framework. This can be best seen when comparing the legal framework of Israel and the Federal Republic of Germany. After World War II, in the light of the atrocities committed by the German people, Germany adopted a legal order that expressed a decisive 'Never again!';[3] and despite attempts of terrorist groups like the 'Rote Armee Fraktion' to disrupt the constitutional order, overall Germany's post-war history is one of prosperity and peace. The result has been a culture that emphasizes the value of human dignity and privacy. Israel, on the other hand, has been under constant threat both by its neighbours and members of its population. Frequent terrorist attacks and a hostile environment have led to a culture that emphasizes security as a prerequisite for the exercise of human rights.[4] Until such a state of security is achieved, certain human rights are deemphasized to a certain extent in order to facilitate the goal of achieving a state of security.[5]

Another example for cultural differences can be found when comparing the United Kingdom and the Federal Republic of Germany. British society is relatively open to technological innovations and seems eager to adopt them, following utilitarian considerations, which leads to an open, liberal and technophile legislature.[6] Germany however can be characterized by the proverbial 'German Angst' which results in scepticism towards technological innovations.[7]

For a more detailed analysis see work package 10 and chapter 2.1.3 of deliverable 9.2 of the SIAM project.

Employee checks

Wherever employees are mandated to pass through security checkpoints – be it on the way to their workplace or even several times over the course of a workday – employees have voiced their dislike of the procedure. Employees feel that – unlike the passengers – they should be trusted by their employers and the state not to maliciously interfere with day-to-day operations. Making employees subject to SMTs means, that they are put under the same type of universal suspicion as passengers

---

3 *Starck*, in: v. Mangoldt/Klein/Starck 2010, Art. 1 Abs. 1 GG, para. 10; *Dreier*, in: Dreier 2013, Art. 1 I GG, para. 41.

4 Cf. Deliverable 9.6 of the SIAM project, 13.

5 An example for this is the fact that in 2009 the state of Israel announced a biometric fingerprint database in which all of its citizens would be enrolled (Biometric Database Law). Cf. Deliverable 9.6 of the SIAM project, 3. Such a database would be considered an immense violation of basic rights in Germany.

6 Cf. the country's attitude towards stem cell research as an example: *Grießler* 2008, 97. Another example is the widespread use of CCTV cameras in the United Kingdom. 1,85 Million CCTV cameras are installed throughout the United Kingdom and every citizen appears approximately 70 times on camera images every day. *Gerrard/Thompson*, CCTVImage 42/2011, 10, 12.

7 *Ronellenfitsch*, JurPC Web-Doc. 115/2007, para. 6.

are. Employees argue that such a practice does nothing to prevent employees for instance from carrying out a terrorist attack. One example is security checks of pilots and crew members in civil aviation. It is argued that a pilot could use the aircraft itself as a weapon in the fashion of the 9/11 attacks at any time he or she wanted to. Thus, there is no need for the pilot to smuggle aboard prohibited items to use them for an attack on the aircraft, since the pilot has command over the aircraft itself.

Nevertheless, in civil aviation security checks of all personnel working in sensitive areas are required by law in the European Union. Additionally, background checks are performed before and during employment in order to sort out all candidates who might be a potential risk to security. More information on the topic can be found in chapter 3.3 of this deliverable.

Data protection

Data protection is both a major issue in the prevention of terrorism and criminal acts through police work and investigations and the on-site prevention of such acts through the use of SMTs.

Many SMTs rely on the collection of personal data; the most prominent perhaps being CCTV and profiling. Despite the importance of the topic of data protection and its prominence in political discussions, data protection in fact seems to be perceived as a burden, a nuisance by those who actually have to consider data protection in day-to-day operations. Some interviewees have thus described data protection as 'annoying'.

Accordingly, the case study reports have revealed that even a major European airport like the Flughafen Berlin Brandenburg which is currently still under construction only offers a part time position (50%) to its data protection officer, whose position the operating company is required by law to maintain.

The interviews also indicate that data protection officers are usually not involved in the early stages of technology acquisition, but are only informed and involved at a later point in time, usually together with employee representatives. A more pro-active role would be highly desirable due to the importance of data protection for the exercise of basic human rights.

As it were, data protection and security seem to be locked in a forced marriage which is nevertheless pivotal to human rights. Making security representatives realize that data protection is more than an obstacle to overcome in order to achieve a minimum compliance with legal standards, is a task that is yet to be completed.

Influence of security actors on legislative processes

With more or less intensity, security actors try to influence legislative processes through lobbying in order to achieve goals that seem desirable to them, like the

reduction of bureaucratic 'red tape' and the elimination of legal norms that restrict or prohibit certain practices that are perceived to have the potential to increase security.

The interviews conducted in this work package indicate that the success rate of such activities is relatively high, making lobbying an attractive tool to achieve one's goals.

Privacy by design

The concept of privacy by design was universally welcomed by the interviewees. Numerous benefits were cited, most prominently the fact that ensuring legal compliance and compatibility prevents financial losses which may result either from having to adapt the technology to a legal framework at a later point in time or the technology being ruled illegal altogether. Legal demands should be identified as early as the design stage. This increases both the legal acceptability as well as the social acceptability of an SMT, since it helps users and passengers to trust the SMT.[8]

However, it seems that in practice privacy by design is not used very often. Some interviewees complained that introducing such a concept will slow down the development process of an SMT, which indicates that the reasons are mainly of an economical nature. Developers eschew the added costs they fear result from concepts like privacy by design, thus failing to realize the economic benefits that are associated with them in the long run.

Responsibility: State vs. Operator

When it comes to the responsibility for the implementation and operation of SMTs, there are four options:

- the state operates public transportation infrastructure and is responsible for security;
- public transportation infrastructure is operated by a private company which is also responsible for maintaining security;
- public transportation infrastructure is operated by a private company, but the state is responsible for security;
- public transportation infrastructure is operated by a private company, but responsibility for security is shared between the operator and the state.

In all four cases, the legislator may or may not have provided instructions for the design of the security regime by mandating legal requirements. Wherever such legal requirements exist, and especially where responsibilities are shared or divided, conflicts of interest may occur. An example will help illustrate this: An airport is operated by a private company, whose primary goal is the maximization of profits. At

[8] See also deliverable 9.2 of the SIAM project on the benefits of considering and including legal requirements as early as during the design phase of SMTs.

the same time, the law dictates that the state is directly responsible for maintaining security at the airport, while the operator is bound by law to assist the state in this effort. In this case, the goal to maximize profits is in conflict with the goal to maintain security, because an extensive and complex security regime is cost-intensive and cuts into the operator's profits since the operator has to provide space for the checkpoints, police stations and other installations.

However, there is also the possibility and potential for partnerships. An example for this is the on-going cooperation between German train operator Deutsche Bahn and the German Federal Police (Bundespolizei): Deutsche Bahn and Federal Police maintain a joint situation room. It has to be noted that Deutsche Bahn AG evolved from Deutsche Bundesbahn and Deutsche Reichsbahn, the state railroads of the Federal Republic of Germany and the German Democratic Republic – nationalized enterprises. Even today, the Federal Republic is the sole proprietor of the Deutsche Bahn AG. In turn, the Federal Police is the successor of the former German railway police (Bahnpolizei). Furthermore, Deutsche Bahn is obligated by law to assist the Federal Police in their efforts to maintain security. These factors may explain the successful and close cooperation between these two partners.

Which party is responsible for security at a site also has a significant effect on the volume and complexity of regulations. In Germany, a private operator will have to rely on his authority as a householder (domiciliary right, Hausrecht) when it comes to security, while a state-run agency may be able to point to a specific set of rules like the German Aviation Security Act that dictates what can and cannot be done.

Informing the public

Informing the public about the use of SMTs has been identified as an aspect of significant importance. In fact, a number of actors in public transportation offer information about SMTs online or through printed materials.

With certain SMTs, legal obligations exist to inform passengers about their use. An example for this is the legal framework regarding the use of surveillance cameras in Germany. Operators are legally required to visibly install signs that clearly indicate that CCTV is in operation.[9] In addition to this, German train operator Deutsche Bahn provides information about security measures via internet, brochures and telephone.

Informing passengers is pivotal to the exercise of passenger rights. Only if passengers are aware of and informed about SMTs in operation, they can make an informed decision whether or not they want to be subjected to these measures. Merely providing passengers with such information on demand is not sufficient for

[9] Cf. § 6b(2) of the German Data Protection Act (Bundesdatenschutzgesetz, BDSG), as well as § 21(3) and (4) of the German Federal Police Act (Bundespolizeigesetz, BPolG).

passengers to be able to fully realize their rights. Rather, informing passengers should be done actively. Such information should include the basic functions and features of the SMTs, directions on forbidden/prohibited items and alternative control measures. The passengers should be made aware of all relevant basic parameters. Language barriers also have to be kept in mind, since travellers with different nationalities may be affected.

Legal evaluation of SMTs – the most relevant criteria

Interviewees were also asked what they consider to be the most relevant and most important criteria when performing a legal evaluation of security measures. In their answers, privacy, data protection and the effects of an SMT on a person's health were highlighted.

However, interviewees also referred to the possibilities of misuse and abuse of SMTs. This indicates that a weighting of the chances and risks that may result from the use of an SMT is a key factor. The term 'chances' is meant to include all potential benefits resulting from the use of an SMT, most notably economic benefits and benefits for security, but also benefits for the exercise of human rights. 'Risks' encompasses all detrimental effects the use of an SMT may have, particularly on human rights.

2.2 Recommendations for interpreting legal requirements

This chapter contains recommendations on how to configure regulations for the proper implementation at the SIAM case study sites and elsewhere.

First however, it has to be noted that the range within which regulations can in fact be interpreted and thus configured is limited. Wherever the wording of an act of parliament or another legal document is unclear and leaves room for interpretation, the four classical methods of legal interpretation may be used. These are:

- grammatical interpretation,
- systematical interpretation,
- historical interpretation, and
- teleological interpretation.

The methods have been described in more detail in chapter 2.1.3 of deliverable 9.2 of the SIAM project.

Still, adhering to these basic methods of interpretation, which are part of the elemental toolkit of any jurist, may not always suffice or lead to the desired outcome, which is to promote and further the protection of human rights and freedoms. Hence, the following recommendations are made, which are the logical

conclusion to the observations made in D9.2 of the SIAM project and during the WP9 case studies.

The recommendations are:

- Permissible deviations from the legal framework (more stringent measures)[10] should be limited as they tend to come with an increased infringement of the basic rights of passengers.

- Where the law does not provide detailed provisions on how to configure the use of SMTs, legal experts should be involved in the design and decision process in order to help realise an approach that respects basic rights.

- Codes of conduct can help to flesh out and to concretise technology-neutral phrases in legal documents.

- Where room for interpretation exists, operators should strive for the interpretation that is most compatible with constitutional requirements.

- Minimum legal requirements should be exceeded in the interest of increasing the legal and social acceptability of an SMT.

- Social aspects and considerations should be taken into consideration, since they can help in the interpretation of legal requirements and in the concretisation of basic rights.

- Where gaps in legal regulations exist, they must be closed through analogy.

- All relevant stakeholders should be involved in the decision process from the start.

In conclusion, it has to be asserted that legal requirements should ideally be integrated into SMTs in the form of CITs. That way an SMT operator does not need to worry about implementing and operating an SMT in accordance with legal requirements; these requirements are automatically fulfilled by choosing appropriate SMTs. This underlines the importance of concepts like Privacy by Design.

[10] Cf. chapter 3.1.4 of this deliverable.

3. Legal regulation as a CIT

The following chapter will look at the effectiveness of legal regulation as a CIT and try to identify potential lacks and opportunities to circumvent regulations. To this end, the European regulations concerning airport security will be depicted and analysed.[11] Subsequently, the same will be done with the legal framework for airport security in Germany and the United Kingdom in order to show exemplarily, how different countries have transformed the European specifications into national law. In the last part, a comparison of these two national approaches will show the freedom of action for the European member states and give an indication if and how this freedom of action can be used or misused in order to deviate from legal requirements set forth by the European Union in the field of airport security.

3.1 Preliminary remarks: The Chicago Convention

The quick development of civil aviation[12] in the first half of the twentieth century made it necessary to develop internationally binding rules. Thus in 1944 the Convention on International Civil Aviation[13] – called Chicago Convention after the place of signature – was created.[14] The document was drafted in the context of an international conference that started on November 1st 1944. It was signed on December 7th 1994 by all 52 participating states. The Federal Republic of Germany joined the Convention in 1956.[15] Up to this day, all member states of the United Nations have signed the Convention.[16] Most current is the ninth edition of the Convention. The purpose of the Convention is according to its preamble to establish generally accepted norms 'in order that international civil aviation may be developed in a safe and orderly manner and that international air transport services may be established on the basis of equality of opportunity and operated soundly and economically'. Thus, the Convention is primarily guided by economic considerations and aimed at guaranteeing the freedom of civil aviation by preventing protectionism while creating common rules and principles. Insofar, the Convention is limited to the field of civil aviation and expressly excludes state operated aircraft, especially military or police aircraft (Art. 3 Chicago Convention). Addressees of the Convention

11 Not including the use of CCTV.

12 Civil aviation encompasses both commercial aviation and the operation of aircraft by private citizens. Following Art. 96 Chicago Convention, commercial aviation can be defined as scheduled air transport conducted by aircraft for the public transportation of passengers, mail or cargo.

13 Convention on International Civil Aviation, Doc 7300 of 7.12.1944.

14 The basis for the creation of the Chicago Convention was the Convention portant Réglementation de la Navigation Aérienne of 1919.

15 Cf. BGBl. 1956 II 411.

16 The only exceptions are Liechtenstein (however, the Convention applies to Liechtenstein nevertheless because of the customs treaty of 1923 with Switzerland) and the Commonwealth nations Tuvalu and Dominica.

are the signatory states which obligate themselves by proxy for those aircraft that operate under their flags and the airports located on their territory. Provisions of the Convention are to be transformed into national law by the signatory states (see Art. 37 Chicago Convention); the Convention is thus a mandate to the signatory states to act.[17] By resolution of April 13 1948 the council of the ICAO declared that a literal transfer of the provisions is desirable.

The Convention is composed of four parts: Part I contains general provisions relating to civil aviation, e.g. the right to use the airspace of a country. Part II creates a distinct authority and constitutes its bylaws. That authority is the International Civil Aviation Organisation (ICAO).[18] Its seat is Montréal, following Art. 45 Chicago Convention, and its aim – as set forth in Art. 44 Chicago Convention – is to 'develop the principles and techniques of international air navigation and to foster the planning and development of international air transport'. Part III governs international air transport, whereas Part IV contains final provisions.

The text of the Convention itself does not contain any provisions relating to the use of security measures. At best Art. 22 Chicago Convention could be considered to be such a provision: 'Each contraction State agrees […] to prevent unnecessary delays to aircraft, crews, passengers and cargo, especially in the administration of the laws relating to immigration, quarantine, customs and clearance.' From this results the requirement to design security checks in a way that does not disturb air traffic. However, since it is up to the signatory states to decide for themselves whether or not a measure amounts to such a disturbance the provision is of little consequence.

The Convention is amended by 18 Annexes. These Annexes serve the concrete implementation of the principles expressed in the Convention; they have to be agreed with by a majority of two thirds of the member of the ICAO Council, the executive organ of the ICAO (Art. 54 lit. l) and Art. 90 Chicago Convention). The Annexes are enacted as 'International Standards and Recommended Practices'. The 'International Standards' are binding while adhering to the latter is merely desirable.[19] Their aim is 'securing the highest practicable degree of uniformity in regulations, standards, procedures, and organization in relation to aircraft, personnel, airways and auxiliary services in all matters in which such uniformity will facilitate and improve air navigation' (Art. 37 Chicago Convention). Art. 37 Chicago Convention also lists the areas in which the ICAO has the power to make provisions.

---

17 This results from the fact that the directives do not directly apply to the signatory states, but first have to be transformed into national law. *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 7. About the effect of international agreements see *Nettesheim*, in: Maunz/Dürig 2012, Art. 59 GG, para. 179 f.

18 It is designed as a special organisation of the United Nations in terms of Art. 57(1) and Art. 63 of the Charter of the United Nations. *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 6.

19 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 7; *Richter* 2013, 23.

Despite the fact that the standards enacted by the ICAO are binding, they have to be understood as minimum standards; according to Art. 38 Chicago Convention signatory states can even go below these standards. However, if a state wants to deviate from the standards he is required to announce these deviations. The ICAO does not have the power to sanction deviations in any way.[20] Still, since 2002 the ICAO from time to time performs audits at international airports and demands rectification if deemed necessary.[21]

In the context of this review, Annex 17 of March 22 1974, titled 'Security - Safeguarding International Civil Aviation Against Acts of Unlawful Interference', including its now 12 amendments is of significant interest. The provisions of Annex 17 were initially aimed at the protection from hijacking and did not apply to domestic flights. With the enactment of the tenth amendment as a reaction to the terrorist attacks of September 11th 2001 the scope was broadened to include domestic flights. On July 1st 2011 the ninth edition of Annex 17 came into force. The document is divided into five chapters. Chapter 1 contains basic definitions, chapter 2 contains basic principles. In chapter 3 the signatory states are requested to create national aviation security programmes, plans and authorities, whereas chapter 4 contains requirements for the use of preventive security measures. It has to be noted that a definition of the term 'security measure' which appears throughout the document is not given. Chapter 5 contains provisions for reacting to unlawful interference[22] with air traffic.

The most important provisions of chapter 4 of Annex 17 which is of significance for this review shall be presented in the following. However, first of all section 2.3 of Annex 17 concretises the provisions of Art. 22 Chicago Convention by recommending that security procedures and controls should be arranged 'to cause a minimum of interference with, or delay to the activities of, civil aviation provided the effectiveness of the controls and procedures is not compromised'. Following section 2.4.1 a contracting state can demand another contracting state to employ additional security measures. The state addressed by such a request has to comply as far as this is practical. Chapter 4 commences by expressing that the ultimate aim of security measures lies in preventing 'weapons, explosives or any other dangerous devices, articles or substances, which may be used to commit an act of unlawful interference, the carriage or bearing of which is not authorized, from being introduced, by any means whatsoever, on board an aircraft engaged in civil aviation' (section 4.1.1). It is recommended to design the use of security measures in a random and unpredictable

20 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 7.

21 For a detailed description of these audits see *Weber*, in: Giemulla/Rothe 2008, 40 ff.

22 For a definition of the term see Annex 17, Chapter 1, Definitions – Acts of Unlawful Interference.

way (section 4.1.2).[23] The subsequent depiction is divided in accordance with the individual areas relevant in the context of aviation security.

Relating to access control (section 4.2) the main aspects are an identity check (section 4.2.3) and a strict separation of landside, airside and security restricted areas (sections 4.2.1 and 4.2.2). Concerning measures relating to aircraft (section 4.3) the main focus lies in preventing unauthorised access to the flight deck (section 4.3.3).[24] However, security measures to secure an empty aircraft before take-off are also prescribed (section 4.3.1). The following sections are concerned with measures relating to passengers and cabin baggage, cargo, mail and other goods like catering (section 4.4 to 4.6), but the provisions are limited to demanding that they must be screened before getting on board the aircraft. There are no statements regarding the type of screening; which thus remains at the discretion of the signatory states. However, every piece of luggage has to be linked to a passenger (section 4.5.5). What follows is an explanation of measures relating to special passenger groups (section 4.7), which primarily means detainees and deportees.[25] This section also contains provisions that allow the use of armed sky marshals (called 'in flight security officers') (sections 4.7.5 and 4.7.7).[26] Concerning measures to secure the landside of airports and concerning cyber security the Annex merely recommends that security measures of some kind need to be taken (sections 4.8 and 4.9).

All in all, Annex 17 merely prescribes basic areas and processes that require the use of security measures in the form of minimum standards. Concrete statements regarding the type of measures to be employed are not made. However, such statements might be included in the Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference.[27] This document can be seen as the implementation manual for Annex 17. It is currently available in 7th edition. However, the manual is not publically available, but only to authorised agencies. A detailed consideration of the manual is thus not possible in the context of this review. What can be said is that especially Volumes III and IV of the manual indeed contain such more detailed statements. Volume III (Airport Security Organization, Programme and Design Requirements) is addressed to airport operators and the

---

23 The reasoning behind this is that 'unpredictability could contribute to the deterrent effect of security measures '.

24 Cf. the provisions of Annex 6, Part I, Chapter 13, Section 13.2 – Security of Flight Crew Compartment.

25 They are described in Annex 17 as 'passengers who are obliged to travel because they have been subject of judicial or administrative proceedings' (cf. section 4.7.1).

26 Only specially trained civil servants are to be used, which excludes granted contractors and other third parties. Secondly, the use of in-flight security officers has to be coordinated with the country of destination. The authorities of the country of destination have to know if and on which flights in flight security officers are used. The pilot in command has to be informed in advance about the use of in-flight security officers including his or her seat. *Weber*, in: Giemulla/Rothe 2008, 44.

27 Aviation Security Manual, Doc 8973.

constructors and planners of airports and contains guidelines concerning airport infrastructure, organisation and design.[28] Volume IV (Preventive Security Measures) on the other hand is addressed to agencies concerned with the implementation of security concepts and contains among other provisions guidelines for access control and luggage screening. However, Volume I (National Organization and Administration) also addresses some topics relevant to aviation security, like the use of in-flight security officers.

3.2 Aviation security regulations in the EU

3.2.1 European Civil Aviation Conference Document 30

1955, eleven years after the signing of the Chicago Convention, the European Civil Aviation Conference (ECAC) was founded in Strasbourg as a permanent organisation of the European aviation administrations[29] and as a European counterpart to the ICAO. The goal of the ECAC is to promote security and efficiency in civil aviation, just as the ICAO does. Seat of the ECAC is Neuilly sur Seine, near Paris. At the same time, the ECAC maintains close ties to the regional bureau of the ICAO in Paris. While the ECAC is an independent organisation, it can nevertheless be seen as a parallel organisation to the ICAO with close connections between the two. The main difference lies in the binding effect of their resolutions: ECAC resolutions are always mere recommendations and thus not legally binding.[30] Currently 44 states are represented as member states in the ECAC, namely all member states of the European Union, but also Norway, Switzerland, Ukraine, Turkey and the states of the Caucasus, not including Russia. Additionally, the European Commission holds the status of spectator in several ECAC committees.

The most important ECAC publication is the 'Manual of ECAC recommendations and resolutions relating to facilitation and Security matters'. This document, whose short name is ECAC Doc. 30, is a summary of all resolutions. It is divided into two parts.

The focus of the first part (ECAC Doc. 30 Part I, currently 11th edition) is not aviation security, but it nevertheless contains a number of provisions relating to security. Section 6.1 states that 'in order to […] ease the processing of hand baggage at security check points and ensure passenger flow […] the amount of hand baggage per passenger on board be limited to one item". In addition to this, Annex 2A contains detailed provisions for the treatment of deportees. Annex 5B has the heading 'Specialist Guidance Material for Security Staff – Key Points for Checks of

28 http://www2.icao.int/en/AVSEC/SFP/Pages/SecurityManual.aspx.
29 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., 1125, para. 8.
30 *Richter* 2013, 29.

Disabled Persons and PRMs[31]' and contains guidelines for security personnel. Page two of Annex 5B begins with the statement that security checks also apply to disabled persons: 'Disabled persons and persons with reduced mobility (PRMs) are not exempt from security checks, but it is important that such checks are carried out carefully and sensitively.' The goal of this provision is to ensure that persons with disabilities are not demeaned by security personnel in any way; that their human dignity is not violated. Thus, page 3 of Annex 5B clarifies: 'Remember to focus on the person, not the disability. All passengers should be treated with respect.' This is concretised in practical guidance, for example: 'It is important that the contents of a blind person's bag are replaced exactly as you found them.'

The second part of ECAC Doc. 30 (currently 8th edition) is not available to the public and thus cannot be discussed here. However, the first European aviation security regulation (2320/2002)[32] is largely based on ECAC Doc. 30 Part II. The successor to this regulation is presented in the following chapter. Thus, ECAC Doc. 30 is of great significance to the use of SMTs in civil aviation, despite the lack of a binding effect and the fact that the document often refers to the standards and recommended practices of the ICAO.

3.2.2 Regulation (EC) No 300/2008

Regulation (EC) 300/2008[33], informally called Civil Aviation Security Regulation, in the following, just like its predecessor, Regulation (EC) No 2320/2002, is aimed at establishing 'common rules to protect civil aviation against acts of unlawful interference that jeopardise the security of civil aviation. It also provides the basis for a common interpretation of Annex 17 to the Chicago Convention on International Civil Aviation.'[34] This indicates that the Regulation is geared to Annex 17 of the Chicago Convention.

On April 29th 2010 Regulation (EC) No 300/2008 replaced Regulation (EC) No 2320/2002.[35] It applies to all civil airports within the European Union (Art. 2(1) of Regulation (EC) No 300/2008) and is addressed to all aviation companies that offer services at these airports. Further addressees are all entities that offer services connected with civil aviation, including suppliers, security firms and flight control.

---

31 Persons with reduced mobility.

32 Regulation (EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security, L 355, 1.

33 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, L 97, 72.

34 Art. 1 of Regulation (EC) No 300/2008. Cf. recitals 1, 2 and 25 of Regulation (EC) No 300/2008.

35 See Art. 24(2) of Regulation (EC) No 300/2008 in conjunction with Art. 4 of Regulation (EU) No 185/2010.

The Regulation aims to regulate all basic principles concerning European aviation security.[36] It contains as the 'mother of all regulations' all fundamental principles of European aviation security law including the legal framework for the enactment of implementing rules.[37] Its predecessor was mostly coextensive with Annex 17 of the Chicago Convention, but was as a regulatory framework amended by detailed provisions, especially the implementing rules of Regulation (EC) No 622/2003. Again, this underlines the importance and relevance of the Chicago Convention, especially its Annex 17, for civil aviation security. However, ECAC Doc. 30, especially Part II, which is in turn based on Annex 17 of the Chicago Convention, also plays an important role.[38] In the course of time, European aviation security law emancipated from these archetypes step by step using margins for interpretation. The fact that there was scope for interpretation meant that before the enactment of the first aviation security regulation there was some fragmentation of national aviation security law between the member states of the European Union, despite the fact that all of them had based their respective national laws on Annex 17. The first aviation security regulation was meant to bring harmonisation by making extensive provisions. Eventually, its successor was enacted to iron out errors and inconsistencies while taking into account experiences made with the old regulation.

The preceding regulation came into being under the impression of the 9/11 attacks[39] and was born by the intention to harmonise aviation security within Europe. At the same time, it was meant to take into account the lessons learned from the events of September 11 2001 and to increase the general level of security in civil aviation. What had previously been regulated only at a national level, flanked by cooperation agreements and Annex 17 of the Chicago Convention, was supposed to be concentrated and centralised in an effective and uniform legal framework.[40] The fact that Regulation (EC) No 2320/2002 was ultimately replaced by Regulation (EC) No 300/2008, resulted from manifold criticism of the original regulation. Structural weaknesses[41] resulting from a legislative process initiated under high political and temporal pressure[42] lead to a regime filled with inconsistencies and redundancies[43].[44] Consequentially, when drafting the successor, more time was

---

36 *Lienhart*, ZLW 1/2009, 1, 8.

37 *Leininger*, ZLW 3/2010, 335, 338.

38 Cf. recital 3 of Regulation (EC) No 2320/2002: The objectives of the regulation 'should be achieved by the adoption of appropriate provisions in the field of air transport policy establishing common basic standards, based on the current recommendations of the European Civil Aviation Conference (ECAC) Document 30.

39 Cf. *Lienhart*, ZLW 1/2009, 1, 1 f.; *Leininger*, ZLW 3/2010, 335, 335 f.

40 *Lienhart*, ZLW 1/2009, 1, 2.

41 For a detailed description of these structural weaknesses see *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 406 f., as well as *Lienhart*, ZLW 1/2009, 1, 4 f.

42 *Lienhart*, ZLW 1/2009, 1, 2. The legislative process was completed in not more than fourteen months.

43 *Leininger*, ZLW 3/2010, 335, 336.

taken to complete the process. In September 2005 the Commission presented a first draft[45], which culminated in Regulation (EC) No 300/2008 in March 2008, after consultations between the European Parliament and the member states concerning the text of the new regulation were on the verge of failing.[46] Compared with its predecessor, the annex is significantly shorter and less detailed.[47] Over-regulation had been identified by the European Commission as one of the reasons for relieving the original regulation.[48]

Regulation (EC) No 300/2008 consists of twenty-four articles and an annex subdivided into twelve sections. The headlines accurately describe the respective contents: airport security, demarked areas of airports, aircraft security, passengers and cabin baggage, hold baggage, cargo and mail, air carrier mail and air carrier materials, in-flight supplies, airport supplies, in-flight security measures, staff recruitment and training, security equipment. The annex can be seen as a first implementation of the provisions of Art. 4 of Regulation (EC) No 300/2008. Accordingly, Art. 4 of Regulation (EC) No 300/2008 – 'common basic standards' – is the core of the regulation. Factually, the provision is a to-do-list that furthermore defines the modalities according to which the necessary measures to fulfil the list may be taken. It has to be emphasised that Art. 4(2) and (3) of Regulation (EC) No 300/2008 allow the European Parliament to exert influence on the constitution of the implementing regulations using the so-called regulatory procedure with scrutiny.[49] This procedure grants the European Parliament a veto right. The reason why the Parliament pushed for this were the experiences made with Regulation (EC) No 1546/2006[50] concerning restrictions for carrying liquids in civil aviation.

---

44 For a detailed presentation of the genesis of Regulation (EC) No 2320/2002 see *Seebohm*, in: Giemulla/Rothe 2008, 24 ff.

45 Proposal for a Regulation of the European Parliament and of the Council on common rules in the field of civil aviation security, COM(2005) 429 final, 2005/0191 (COD).

46 Particularly the question of financing security measures proved to be a significant stumbling block. *Lienhart*, ZLW 1/2009, 1, 5 f., 10 f. The question of finance was the reason, why it took until 2010 for Regulation (EC) No 2320/2002 to be replaced by its successor. Cf. *Leininger*, ZLW 3/2010, 335, 343 f.

47 18 pages compared to four pages.

48 COM(2005) 429 final, 2.

49 Thus Regulation (EC) No 272/2009 is also called 'PRAC regulation'. PRAC = Procédure de Réglementation Avec Contrôle. See also Art. 19(3) of Regulation (EC) No 300/2008. The procedure was introduced by the Council Decision of 17 July 2006 amending Decision 1999/468/EC laying down the procedures for the exercise of implementing powers conferred on the Commission (2006/512/EC). It has to be kept in mind however, that Regulation (EU) No 185/2010 is not affected by this, which was instead enacted following the committee procedure as laid down in Art. 19(2) of Regulation (EC) No 300/2008. *Leininger*, ZLW 3/2010, 335, 340. The commission procedure is a procedure where decisions are made by the Regulatory Committee which consists of experts from the ministerial bureaucracy of the member states. *Leininger*, ZLW 3/2010, 335, 336.

50 Commission Regulation (EC) No 1546/2006 of 4 October 2006 amending Regulation (EC) No 622/2003 laying down measures for the implementation of the common basic standards on aviation security, L 286, 6.

Parliament, which had not been involved in the enactment of that regulation, now demanded a bigger right to say in questions of aviation security.[51]

Deviations from the basic standards found in Art. 4 of Regulation (EC) No 300/2008 are possible within the boundaries of Art. 4(4)(1) of Regulation (EC) No 300/2008. Thus, member states can introduce alternative security measures. The precise circumstances that allow such a deviation can be found in a confidential Decision[52].[53] The framework for the use of more stringent measures can be found in Art. 6 of Regulation (EC) No 300/2008 and stipulate an anticipatory risk analysis of the measures.[54] Following Art. 6(1)(2) the more stringent measures 'shall be relevant, objective, non-discriminatory and proportional to the risk that is being addressed'. In case of any deviation the member states are required to notify the Commission, except 'where the measures concerned are limited to a given flight on a specific date' (Art. 6(3) of Regulation (EC) No 300/2008). The possibility to deviate results from the principle of subsidiarity, but is also owed to the acknowledgement that between the member states different risk evaluations exist which means that individual states must be allowed the possibility to go beyond what is required by European law.[55]

Another central aspect is the requirement of Art. 10 of Regulation (EC) No 300/2008 that every member state has to set up and apply a national civil aviation security programme. Similar security programmes have to be drawn up by airport operators (Art. 12(1) of Regulation (EC) No 300/2008), air carriers (Art. 13(1) of Regulation (EC) No 300/2008) and other entities required by the national programmes 'to apply aviation security standards' (Art. 14(1) of Regulation (EC) No 300/2008).

Art. 13(3) of Regulation (EC) No 300/2008 is the basic pillar for 'one stop security' within the European Union. 'One stop security' means waiving any rechecks of transit passengers and cargo whose point of origin is considered secure.[56] Following Art. 13(3) of Regulation (EC) No 300/2008 all member states must recognise the security concept of a Community air carrier which 'has been validated by the appropriate authority of the member state granting the operating licence'. This means, however, that any non-Community air carrier is in principle except from the

---

51 *Leininger*, ZLW 3/2010, 335, 339.

52 Commission Decision C(2010)774.

53 *Leininger*, ZLW 3/2010, 335, 342.

54 Especially the United Kingdom has used this possibility to introduce more stringent measures. *Seebohm*, in: Giemulla/Rothe 2008, 26.

55 *Seebohm*, in: Giemulla/Rothe 2008, 26.

56 Cf. recital 20 of Regulation (EC) No 300/2008: 'The goal of 'one-stop security' for all flights within the European Union should be advanced.' and recital 21: 'it should not be necessary to rescreen passengers or their baggage arriving on flights from third countries that have aviation security standards equivalent to those laid down by this Regulation.'

concept of 'one stop security'.[57] Exceptions exist where an agreement between the European Union and a third country has been made that recognises the equivalency of the security standards in the third country. Besides bilateral agreements[58] a unilateral recognition of an equality of security standards is possible (Art. 4(2)(e) of Regulation (EC) No 300/2008 in conjunction with Part E of the Annex of Regulation (EC) No 272/2009).[59] However, it is possible to take away the privilege to take part in the 'one stop security' concept even within the European Union. This is the case where during an inspection of an airport severe shortcomings are detected (so-called 'Art. 15 procedure'). Until these shortcomings are overcome, the respective airport is considered 'unclean' and any passengers, luggage and freight coming from that airport have to be rechecked. All in all, it has to be asserted that the implementation of 'one stop security' is moving forward rather slowly.

Since Regulation (EC) No 300/2008 is a framework regulation which requires concretisation through implementing regulations, its provisions are of a general nature. Thus, Regulation (EC) No 300/2008 generally demands 'appropriate measures' or 'appropriate security measures'.[60] Other provisions are worded in an equally open and general way and merely demand that security measures have to be applied to protect certain areas, objects or processes. One example for this is 5.1(1) of the Appendix of Regulation (EC) No 300/2008 where the regulation contains the following provision concerning hold baggage: 'All hold baggage shall be screened prior to being loaded onto an aircraft in order to prevent prohibited articles from being introduced into security restricted areas and on board aircraft.' Indications for the type of the screening are not provided. Such provisions are only included in the regulations and decisions reviewed in the following chapters.

Further terms of regulation – besides the basic Where and If of security measures – are for instance the right of the Commission following Art. 15 of Regulation (EC) No 300/2008 to check up on compliance with the provisions for aviation security within the member states. Violations are made public and sanctions are imposed on the violating party. Moreover, the regulation demands a partition of airports into parts with different levels of security. Airports are to be divided into a landside and an airside. Security restricted areas are to be established on the airside. Following Art. 3(11) of Regulation (EC) No 300/2008 the airside of an airport is defined as 'the movement area of an airport, adjacent terrain and buildings or portions thereof, access to which is restricted'. Security restricted areas are defined by Art. 3(13) of Regulation (EC) No 300/2008 as 'that area of airside where, in addition to access

---

57 *Leininger*, ZLW 3/2010, 335, 345.

58 Such an agreement exists between the European Union and the United States of America. However, the USA do not recognize European airports as being secure.

59 *Leininger*, ZLW 3/2010, 335, 348.

60 In 3(1), 4.3, 5.3, 10(1)(b), 10(2), 11(1), 12 of the Appendix of Regulation (EC) No 300/2008.

being restricted, other aviation security standards are applied'. All remaining areas of an airport form the landside. Within security restricted areas, so-called 'critical parts' have to be accounted for. Additionally, the regulation demands background checks of persons who have unescorted access to security restricted areas using either a crew identification card or an airport identification card (1.2(4) of the Appendix of Regulation (EC) no 300/2008).[61] Furthermore personnel are to be screened for prohibited items and have to have their identity checked (1.3 of the Appendix of Regulation (EC) No 300/2008), meaning that personnel has to endure similar security measures if operating in sensitive areas of an airport.

In addition to security measures on the ground, measures during flight are also addressed. They can be found in chapter 10 of the Appendix of the regulation. As an example for such security measures, 10(2) of the Appendix of Regulation (EC) No 300/2008 names 'training of flight crew and cabin staff' to 'prevent acts of unlawful interference during a flight'. As a reaction to the events of September 11 2001, the cockpit is to be protected from unauthorised entry (10(1)(a) of the Appendix of Regulation (EC) No 300/2008). More detailed provisions for in-flight security measures have not been enacted up to today.[62] The member states are free in their decision whether or not to use so-called 'sky marshals' (Recital 8 of Regulation (EC) No 300/2008).

3.2.3 Commission Regulation (EC) No 272/2009

As indicated by its full title[63], the purpose of Regulation (EC) No 272/2009 is to amend the provisions of Regulation (EC) No 300/2008 by implementing the requirements set forth in Art. 4(2) of Regulation (EC) No 300/2008. The regulation consists of not more than three articles and an annex partitioned into eleven parts. These parts of the annex – A to K – correspond to Art. 4(2)(2)(a) to (k) of Regulation (EC) No 300/2008. For the use of security measures, parts A, B and D are of particular interest.

Part A lists the accepted screening methods for the screening of persons, cabin baggage, liquids[64], hold baggage, cargo and mail, as well as air carrier mail and air carrier materials. In the following, the provisions of part A.1 which are concerned with the screening of persons will be presented as an example. For the screening of

---

61 Such a background check includes an identity check and a review of criminal record and covers 'employment, education and any gaps' (11.1.3 of the Appendix of Commission Regulation (EU) No 185/2010).

62 The corresponding chapter 10 of Commission Regulation (EU) No 185/2010 is empty.

63 Commission Regulation (EC) No 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council, L 91, 7.

64 This encompasses liquids, aerosols and gels (short: LAGs).

persons it is allowed to use hand searches, walk-through and hand-held metal detection equipment, explosive detection dogs, explosive trace detection equipment and security scanners.[65] These SMTs do not need to be used cumulatively, but have to be understood as a catalogue of alternative measures that can be used 'individually or in combination, as a primary or secondary means'.[66] This means that these measures are options. It also means that only the basic type of an SMT is predetermined by the regulation, whereas provisions concerning technologies and processes are not to be found in the regulation. Security scanners shall serve as an example to illustrate this. The regulation merely determines that only scanner using non-ionising radiation may be used. It does not determine that a certain scan method has to be used (for instance millimetre or Terahertz radiation), but merely excludes x-radiation from being used. Part D amends the provisions of Part A by listing measures allowed for the screening of aircraft and vehicles.

The lists that can be found in parts A and D are thus of great significance for the use of SMTs in civil aviation as they determine which types of measures are allowed for certain types of security checks. Part B contains yet another list that is of great importance, which is the list of articles that a SMT from the 'detection' category has to be capable of detecting reliably in order to meet the demands of day-to-day operation.

Part C of the annex contains basic provisions for access to security restricted areas. Furthermore, the regulation contains the legal framework of the recognition of third countries as 'clean' in relation to the concept of 'one stop security' (part E of the annex), as well as provisions for the screening of cargo, mail, air carrier mail, air carrier materials, in-flight supplies and airport supplies[67] (parts F, G, and H of the annex). The concluding parts of the annex are concerned with the criteria for defining 'critical parts' of security restricted areas (part I), staff recruitment and methods of training (part J) and conditions for special security procedures and exemptions from security controls (part K). In summary, it has to be concluded that the provisions of Commission Regulation (EC) No 272/2009 require further concretisation. This concretisation takes place in the legal acts reviewed in the following chapter.

---

65 Security scanners were added to the list by Commission Regulation (EU) No 1141/2011 of 10 November 2011 amending Regulation (EC) No 272/2009 supplementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports.

66 Part A of the Annex of Commission Regulation (EC) No 272/2009.

67 For definitions of these terms cf. Art. 2 of Commission Regulation (EC) No 272/2009.

3.2.4 Commission Regulation (EU) No 185/2010 and Commission Decision C(2010)774

Commission Regulation (EU) No 185/2010[68] as well as Commission Decision C(2010)774[69] are aimed at 'laying down detailed measures for the implementation of the common basic standards on aviation security'. Thus, both primarily serve the implementation of Art. 4(3) of Regulation (EC) No 300/2008. The splitting of the implementation of Art. 4(3) of Regulation (EC) No 300/2008 into two separate documents, results from the necessity to keep certain provisions relating to aviation security secret, in order to avoid handing information to attackers that might help them circumvent security measures. As a result, Commission Decision C(2010)774, which contains among others provisions for the technological effectiveness of security measures[70], has been branded classified information within the meaning of Commission Decision 2001/844/EC, ECSC, Euratom[71], following Art. 18(a) of Regulation (EC) No 300/2008.[72] What follows is a division of the 'detailed measures' into a public part (Commission Regulation (EU) No 185/2010) and a non-public part (Commission Decision C(2010)774) which may 'be made available to those operators and entities with a legitimate interest'.[73]

The predecessor of Commission Regulation (EU) No 185/2010, which was enacted using the committee procedure, was Commission Regulation (EC) No 820/2008[74]. The predecessor of that regulation was Commission Regulation (EC) No 622/2003[75]. The reason why it was replaced was the case *Gottfried Heinrich*[76]. The judgment summarises the facts of the case as follows: 'That reference was submitted in the course of an action brought by Mr Heinrich against the Austrian authorities after they had refused him access on board an aeroplane on the ground that he was carrying tennis racquets in his cabin baggage, those objects being regarded by those

---

68 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 L 55, 1.

69 Commission Decision C(2010)774 final of 13 April 2010 laying down detailed measures for the implementation of the common basic standards on aviation security containing information as referred to in Point (a) of Article 18 of Regulation (EC) No 300/2008. This includes Commission Decision C(2010)2604 final of 23 April 2010 amending Commission Decision 2010/774/EU of 13 April 2010 laying down detailed measures for the implementation of the common basic standards on aviation security containing information as referred to in Point (a) of Article 18 of Regulation (EC) No 300/2008.

70 For instance performance requirements for metal detector gates. *Leininger*, ZLW 3/2010, 335, 340.

71 Doc. No C(2001)3031.

72 Cf. recital 16 of Regulation (EC) No 300/2008.

73 Recital 16 of Regulation (EC) No 300/2008.

74 Commission Regulation (EC) No 820/2008 of 8 August 2008 laying down measures for the implementation of the common basic standards on aviation security, L 221, 8.

75 Commission Regulation (EC) No 622/2003 of 4 April 2003 laying down measures for the implementation of the common basic standards on aviation security, L 89, 9.

76 ECJ, judgment of March 10 2009, C-345/06

authorities as articles prohibited by an unpublished annex to a civil aviation security regulation.'[77] Commission Regulation (EC) No 622/2003 contained the list of articles that were not allowed aboard aircraft. The list was classified, just as the regulation as a whole which meant it was inaccessible to the public. In April 2008, during the proceedings, advocate general *Sharpston* demanded the regulation to be declared inexistent in a legal sense by the court due to a violation of formal requirements set forth by Art. 254(2) of the Treaty of Rome.[78] Fearing the court would follow that demand, Commission Regulation (EC) No 622/2003 was replaced by Commission Regulation (EC) No 820/2008, which was published in the official journal[79], in August 2008. Provision that were to remain classified were put into Commission Decision C(2008)4333[80]. That decision is in turn the predecessor of Commission Decision C(2010)744. These events explain the division of the implementation of Art. 4(3) of Regulation (EC) No 300/2008 into two documents out of which one has been designated as classified while the other was published in the official journal as usual. This practice could become a model for the further development of aviation security law.[81] Art. 18 of Regulation (EC) No 300/2008 indicates which provisions are published and which are kept secret: 'the Commission shall publish measures that have a direct impact on passengers.' This follows from the *Heinrich* case which lead to the realisation that passengers must be allowed access to provisions that directly concern them.

The following paragraph will give an overview of the most relevant provisions of Commission Regulation (EU) No 185/2010. The regulation consists of just four articles and an extensive annex, which is divided into twelve chapters. The organisation of the annex is consistent with the annex of Regulation (EC) No 300/2008; the twelve chapters have the same headings as the annex of Regulation (EC) No 300/2008. Thus chapter 1 is concerned with airport security. Chapter 1.1 concretises the provision relating to the establishing of security restricted areas (1.1.2.1)[82] and critical parts of security restricted areas (1.1.3.2)[83]. Ultimately, this

---

77 See para. 2 of the judgment.

78 *Lienhart*, ZLW 1/2009, 1, 7 f.

79 L 211, 8.

80 Commission Decision C(2008)4333 final of 8 August 2008 laying down additional measures for the implementation of the common basic standards on aviation security.

81 *Lienhart*, ZLW 1/2009, 1, 8.

82 A security restricted area is 'a part of an airport to which screened departing passengers have access' (1.1.2.1(a)), 'a part of an airport through which screened departing hold baggage may pass or in which it may be held' (1.1.2.1(b)), and 'a part of an airport for the parking of aircraft to be boarded or loaded' (1.1.2.1(c)).

83 Critical parts are 'all parts of an airport to which screened departing passengers have access' (1.1.3.2(a)) and 'all parts of an airport through which screened departing hold baggage may pass or in which it may be held' (1.1.3.2(b)). Maintenance areas and parking spaces for aircraft are exempt. Following 1.0.2 'an aircraft, bus, baggage cart or other means of transport, or a walkway or jetway shall be regarded as a part of an airport' and thus also count as security restricted areas and critical parts. *Leininger*, ZLW 3/2010, 335, 350 f.

decides the points of use of SMTs, since these areas have to be separated by security checks from other areas of the airport. Under heading 1.2.2.2 the requirements can be found that allow a person to enter a security restricted area. A person must present boarding card, a crew identification card, an airport identification card or a card of a relevant authority. There must be suitable security measures in place to ensure that these cards are valid and correspond to the holder. When checking the validity of the boarding card, a mere visual inspection is deemed sufficient, at least where the card is not machine-readable. However, it has to be kept in mind, that an attacker can easily purchase a valid boarding card. *Leininger* thus states that it is unreasonable to assume that an attacker might be deterred by the fact that a boarding pass is required to enter security restricted areas of an airport.[84] This puts the effectiveness of checking boarding passes as a security measure into question. The main purpose of this seems to be maintaining economic interests. Vehicles that enter security relevant areas have to display a valid vehicle pass. When entering critical areas, 1.4.1.1 stipulates that vehicles have to be examined. Commission Decision C(2010)744 contains a quota for random checks, as well as the parts of a vehicle that have to be searched during such a check.

An important factor for access control is the fact that certain areas of an airport are used by arriving as well as departing passengers, e.g. the jetways. This means that passengers arriving from 'unclean' airports could access critical parts of security relevant areas and leave behind objects in the areas. Such objects, e.g. an explosive device, could be left behind or handed to an accomplice who then takes it aboard an aircraft for detonation. In order to prevent this and similar scenarios, security relevant areas and critical parts need to be searched 'in order to reasonably ensure that it does not contain prohibited articles'.[85] In practice such a search will usually consist of a visual examination of the area including doors, covers, shelves etc.[86] 1.5.1 eventually contains the framework for all surveillance, patrols and other physical controls.[87]

Chapter 3 is concerned with aircraft security. A key element is the so-called 'aircraft security search' which means that any aircraft arriving from a third country has to be searched for prohibited articles after all passengers have embarked and all freight has been unloaded. Thus, aircraft are differentiated by their point of origin.[88] Again, detailed provisions for the searches, including those areas of an aircraft that must be searched, can be found in Commission Decision C(2010)744. Parked aircraft have to

---

84 *Leininger*, ZLW 3/2010, 335, 352.

85 See 1.1.2.2, 1.1.2.3, 1.1.3.3 and 1.1.3.4.

86 *Leininger*, ZLW 3/2010, 335, 351 f.

87 1.5.2: 'The frequency and means of undertaking surveillance and patrols shall be based on a risk assessment undertaken by the appropriate authority'.

88 *Leininger*, ZLW 3/2010, 335, 358.

be secured against unauthorised access (3.2.1.1). The simplest measure to ensure this would be to simply lock all access doors. Another possibility would be the use of electronic access detection systems. Any person who wants to access an aircraft needs to be able to present legitimation for doing so. This creates another, separate layer of security within critical parts of security restricted areas, since being granted access to an area where an aircraft is parked does not include authority to enter the aircraft.

Chapters 4 and 5 are of key significance for checks of passengers and their luggage[89]. The primary goal of these checks is to prevent dangerous objects from getting aboard an aircraft. This makes it necessary to first create a list of those items that a security check must be able to detect. Attachment 4-C of the Annex contains such a list of 'prohibited articles'. However, the use of the word 'including' reveals that the articles found in the list are merely examples, meaning that the list is not exclusive. In contrast to its predecessor, the list only contains articles that can cause 'serious injury', but not articles that are generally capable of causing any kind of injury. This change mainly concerns sports equipment. Thus, the tennis racket that provoked the *Heinrich* case and ultimately lead to the declassification of the list would today not be considered a prohibited article. The SMTs that are allowed for passenger screening have already been listed in the previous chapter. Commission Regulation (EU) No 185/2010 contains provisions concerning the use of these SMTs. These provisions are further defined in Commission Decision C(2010)744. For instance, 4.1.1 of the Regulation is related to the screening of passengers using walk-through metal detection equipment. Sections 4.1.2 to 4.1.4 of the Annex of Commission Decision C(2010)744 further refine this by stipulating quotas for random passenger screening with such equipment. Knowledge of these quotas could be used for attempts to circumvent security checks, which means that they had to be put into the classified Decision and not into the public Regulation. The same is true for the structure of the provisions concerning the screening of both cabin and hold baggage. The following provisions, which in their entirety form the screening mechanism that has become a routine for any airline passenger, deserve special mention. Following 4.1.1.1, 'coats and jackets of passengers shall be taken off and shall be screened as cabin baggage'. Following 4.1.2.1, 'portable computers and other large electrical items shall be removed from cabin luggage and shall be screened separately'. Section 4.1.3 contains provisions for the screening of liquids.[90] Eventually, section

[89] Provisions for checking persons that are not passengers and articles carried by them can be found in 1.3 of Commission Regulation (EU) No 185/2010.

[90] Newly edited by Commission Implementing Regulation (EU) No 246/2013 of 19 March 2013 amending Regulation (EU) No 185/2010 as regards the screening of liquids, aerosols and gels at EU airports.

4.1.1.10, which was introduced by Commission Implementing Regulation (EU) No 1147/2011[91], contains provisions for the use of body scanners.

Chapters 5 and 6 are concerned with the screening of checked baggage, cargo and mail, meaning all items that are transported in the cargo hold of an aircraft. These items are primarily screened using x-ray machines, devices for trace explosives detection and sniffer dogs. Due to technological advances, pieces of luggage do not necessarily have to be unloaded and screened again when a passenger whose baggage has already been loaded into the cargo hold does not make his or her flight (unaccompanied baggage)[92].[93] This results from section 5.3.2 in conjunction with section 5.3.3[94], which stipulate that unaccompanied baggage may only be transported if it has be subjected to suitable security measures or where it was separated from the respective passenger without his or her fault. In the past, the principle of unloading unaccompanied baggage was treated like a dogma.[95]

Both, the screening of persons and the screening of objects, can be divided into two tiers. The first tier is there to ensure that persons, baggage and cargo are sufficiently screened. In the second tier, the 'secure' area that lies beyond the security checkpoints has to be protected in order to prevent unauthorised entry of persons and unauthorised insertion of objects.

Chapters 7 to 12 will not be discussed in much detail in this review. Chapters 7 to 9, just like their counterparts in Regulation (EC) No 300/2008 and Commission Regulation (EC) No 272/2009, are concerned with air carrier materials and mail, in-flight supplies, and airport supplies. Instead of a detailed review, the comments on cargo and mail can be referred to. Chapter 10 is empty, as mentioned above, whereas chapter 11 is concerned with staff recruitment and training. Chapter 12 contains provisions regarding security equipment. The bulk of these provisions concerns safe operation of security equipment, like for instance the provision that metal detector gates 'shall be firmly fixed to a solid base' (12.1.1.3). However, chapter 12 also contains performance requirements for certain SMTs. For instance, devices for screening liquids must be capable of detecting dangerous contents 'independent of the shape or material of the LAG container' (12.7.1.2). More

---

91 Commission Implementing Regulation (EU) No 1147/2011 of 11 November 2011 amending Regulation (EU) No 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airports.

92 Art. 3(21) of Regulation (EC) 300/2008 defines accompanied hold baggage as 'baggage, carried in the hold of an aircraft, which has been checked in for a flight by a passenger travelling on that same flight'.

93 If hold luggage 'becomes unaccompanied baggage due to factors other than those mentioned in point 5.3.2' it still has to 'be rescreened after removal from the aircraft and before loading it again' (section 5.3.3.2).

94 Cf. Section 5.3(2) of the Annex of Regulation (EC) 300/2008.

95 *Leininger*, ZLW 4/2010, 485, 509.

concrete requirements can only be found in the classified Commission Decision C(2010)744. Section 12.8 which contains provision for the use of new technologies deserves special mention. Their use is allowed 'for the purpose of evaluating a new method of screening' (12.8.1(a)). The maximum duration of such a test is thirty months (12.8.7).

In conclusion, it can be said that there is a division of labour between Commission Regulation (EU) No 185/2010 and Commission Decision C(2010)744 which was born out of necessity, namely as a result of the *Heinrich* case. Nevertheless, both legal acts have to be understood as a unity. One cannot be considered without the other.

3.2.5 Commission Regulation (EU) No 1254/2009

Exemptions from the security standards set forth in Regulation (EC) No 300/2008 are possible. Commission Regulation (EU) No 1254/2009[96] which consists of only two articles states in Art. 1 that an airport is exempt if air traffic is limited to small aircraft that weigh less than 15 t or limited to flights in the context of law enforcement, fire suppression or providing medical or humanitarian aid. Furthermore, airports or individual parts of an airport are exempt that are only used for testing, research or development. The exemptions also apply where neither passengers, nor baggage, cargo or mail are transported, and they apply to small aircraft (less than 45,4 t) that are used 'for the carriage of own staff and non fare-paying passengers or goods as an aid to the conduct of company business'. Here, the member states are given significant leeway.[97] The reasoning behind this is that the dangers that such airports pose to aviation security are considered to be negligible.[98]

---

96 Commission Regulation (EU) No 1254/2009 of 18 December 2009 setting criteria to allow Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures.

97 Cf. *Leininger*, ZLW 3/2010, 335, 357 f.

98 However, an incident on January 1st 2003, during which a mentally ill man hijacked a motor glider at gunpoint at Babenhausen airport, puts the validity of this argument into question. The hijacker circled over Frankfurt am Main for about two hours, threatening to commit suicide by crashing the aircraft into a skyscraper in order to commemorate astronaut *Judith Resnik* who was killed in 1986 in the space shuttle Challenger disaster. The authorities were able to persuade the pilot to land the aircraft at Frankfurt am Main airport. It is assumed that crashing the aircraft would have resulted in only minor damage. *Esslinger, D.*, Liebesgrüße nach Baltimore, Süddeutsche Zeitung, Deutschland, Bayern, München, Die Seite Drei, 7.1.2003. The incident greatly influenced the enactment of the German Aviation Security Act (see below). *Richter* 2013, 73. In a similar incident, on 5.1.2002 a student (15) flew a stolen Cessna 172 into a skyscraper in Tampa, Florid thus committing suicide. The resulting damage to the building was minimal. Apart from the pilot, no other person was harmed. *Wald, M. L.*, Student Pilot, 15, Crashes Plane Into Tower in Flordia, The New York Times, 6.1.2002, U.S.

3.2.6 EU OPS

Council Regulation (EEC) No 3922/91[99] (short: EU OPS[100]) mostly deals with technical requirements and specifications of aircraft and is thus mainly concerned with safety, not security. Nevertheless, Subpart S of the third annex of the Regulation contains some provisions relating to aviation security. The measures described in Annex III Subpart S OPS 1.1255 for securing the cockpit deserve particular mention. The cockpit door 'shall to be capable of being locked', while the cabin crew has to be given means to 'notify the flight crew in the event of suspicious activity or security breaches in the cabin'.[101] Further provisions apply only to larger aircraft[102]: The cockpit door must be 'capable of being locked and unlocked from each pilot's station'.[103] The cockpit crew must be able to monitor the area outside the flight compartment 'to the extent necessary to identify persons requesting entry to the flight compartment and to detect suspicious behavior or potential threat'.[104] The regulation recommends keeping cockpit doors locked at all times during flight, but leaves the final decision to the aircraft commander of national provisions.[105]

3.2.7 Council Directive 2004/82/EC

Council Directive 2004/82/EC[106] obligates air carriers to transmit certain information about the passengers they transport. The transmission of data occurs on request of those national agencies that are responsible for performing identity checks at the external frontiers of the Community.[107] Art. 3(2) of the Directive contains a list of the information that have to be transmitted on request: the number and type of travel document used, nationality, full names, date of birth, the border crossing point of entry into the territory of the Member States, code of transport, departure and arrival time of the transport, total number of passengers carried on that transport, and the initial point of embarkation. These information must be deleted after 24 hours (Art. 6(1) of the Directive). The main purpose of the Directive is 'improving

99 Council Regulation (EEC) No 3922/91 of December 1991 on the harmonization of technical requirements and administrative procedures in the field of civil aviation, L 373, 4.

100 OPS stands for Operations.

101 Annex III Subpart S OPS 1.1255(a).

102 More than 45,5 t or more than 60 passenger seats.

103 Annex III Subpart S OPS 1.1255(b).

104 Annex III Subpart S OPS 1.1255(c)(2).

105 '[…] when required by security procedure of the commander.' Annex III Subpart S OPS 1.1255(c)(1).

106 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, L 261, 24.

107 This is contrasted by the so-called Passenger Name Record Agreement between the European Union and the United States of America where data is transmitted by default, not on request; push vs. pull (Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security, 17434/11).

border controls and combating illegal immigration'.[108] Thus, the directive only applies to flights from third countries to a member state of the European Union (Art. 3(1) of the Dircetive). Using the information for any other purpose is only allowed if these purposes are related to the duties of the national authority responsible for border control. It has to be concluded that the transmission of data is not a security measure directly aimed at combating terrorism[109], but instead limited to illegal migration. Nevertheless, it may provide an additional benefit for combating terrorism as a side effect.[110]

3.2.8 Regulation (EC) No 1107/2006

Regulation (EC) No 1107/2006[111] is concerned with the rights of disabled passengers and demands providing special assistance for those passengers in order to enable them to partake in civil aviation. This has an effect on the use of SMTs. Annex I makes it clear that 'assistance and arrangements' must be made 'to enable disabled persons and persons with reduced mobility to […] customs and security procedures'. Thus STMs must be designed in a way that disabled persons can pass through them or alternative measures must be provided. This is an implementation of Art. 26 of the Charter of Fundamental Rights of the European Union.

3.2.9 Summary

The review of European aviation security law has revealed that a regulatory structure was chosen that consists of several levels of concretisation. While the framework regulation is worded in a very general way, the provisions become more and more concrete with every level. The highest level of concretisation can be found in Commission Decision C(2010)774. However, this decision could not be reviewed in detail due to the fact that it is classified. European aviation security law is divided into a framework regulation (Regulation (EC) No 300/2008), a basic implementing regulation (Commission Regulation (EC) No 272/2009) and public (Commission Regulation (EU) No 185/2010) as well as classified detailed implementing regulations (Commission Decision C(2010)774).[112]

---

108 Art. 1 of the Directive. Cf. *van Schyndel*, in: Giemulla/Rothe 2008, 11. This appropriation is another difference between the above-mentioned PNR Agreement and the Directive.

109 *van Schyndel*, in: Giemulla/Rothe 2008, 16.

110 *Drewes/Malmberg/Walter* 2010, § 31a BPolG, para. 2.

111 Regulation (EC) No 1107/2006 of the European Parliament and of the Council of 5 July 2006 concerning the rights of disabled persons and persons with reduced mobility when travelling by air, L 204/1.

112 *Leininger*, ZLW 3/2010, 335, 340.

However, despite the provisions contained in these legal acts, significant leeway remains for the member states. First, member states have the right to implement more stringent measures, which means they can use measures that are not contained in the European provisions. Second, the provisions of the annex of Commission Regulation (EC) No 272/2009, and particularly parts A and D, are flexible, since the lists contained there have to be understood as a string of alternatives. A member state may choose from the lists those measures that he regards most suitable. When making that choice, the effects of individual and cumulative measures on the rights of the passengers should be kept in mind. Furthermore, the alternative options themselves give leeway, since concrete technologies for instance for explosives trace detection are not stipulated.

3.3 Aviation security regulation in Germany

In Germany, the legal provisions concerning aviation security are concentrated in the German Aviation Security Act (Gesetz zur Neuregelung von Luftsicherheitsaufgaben, LuftSiG) of January 11 2005.[113] Prior to this act, the provisions on aviation security were scattered over a multitude of acts.[114] The law was enacted by the federal government (Bund) which is the responsible authority for enacting civil aviation law[115] due to the provisions of Art. 71(1)(6) of the German Basic Law.[116] The act is based mainly on Regulation (EC) No 2320/2002, the predecessor of the current Civil Aviation Security Regulation (Regulation (EC) No 300/2008).[117] The reason why the law had to be enacted lies in the fact that the Civil Aviation Security Regulation does not contain any provisions regarding specific responsibilities on a national level; and indeed it could not, due to the national differences within the European Union. Furthermore, the explanatory memorandum explicitly refers to the terrorist attacks of September 11 2001 and an event in 2003 where a motor glider circled over Frankfurt/Main.[118] Different scenarios relating to attacks on civil aviation that ultimately cannot be conclusively evaluated required in the eyes of the federal government the creation of clear-cut responsibilities both at federal and state level in order to establish a quick and efficient structure for information sharing and

113 BGBl. 2005 I 78.

114 Bundestag printed paper 15/2361, 14; *Richter* 2013, 73 f.; *Faust/Lienhart*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 61; *Giemulla*, in: Giemulla/van Schyndel 2006, § 1 LuftSiG, para. 1.

115 This encompasses all areas related to civil aviation including the operation of airports and the defence against specific threats. *Uhle*, in: Maunz/Dürig 2012, Art. 73 GG, para. 135 ff.

116 For an explanation of doubts that the Bund is in fact the competent authority and for a description of the turbulent history of the German Aviation Security Act see *Richter* 2013, 74 ff.

117 For a detailed depiction of the history of German aviation security law see *Giemulla*, in: Giemulla/van Schyndel 2006, Section 1 'Allgemeines', para. 17 ff.

118 Bundestag printed paper 15/2361, 2.

decision making.[119] From the hierarchy of European aviation security law with the directly applicable Civil Aviation Security Regulation on top follows that the German LuftSiG may only amend European law, but not change or restrict it.[120] Thus the main goal of the LuftSig is to close any gaps left behind by the Civil Aviation Security Regulation and connected European law and to adapt national law to the Civil Aviation Security Regulation; especially since the Civil Aviation Security Regulation contains a multitude of obligations without naming addressees.[121] This means that these 'open obligations' had to be connected to concrete addressees.[122] Additionally, the legislator wanted to create a legal basis for shooting down civil aircraft as a reaction to the events in 2001 and 2003. The LuftSiG is part of the German National Aviation Security Programme as demanded by Art. 10 of the Civil Aviation Security Regulation.[123] § 1 LuftSiG states the protection from threats against the security of civil aviation, especially hi-jackings, sabotage and terrorist attacks as the aim of the act.

Ever since 1980, German aviation security is based on the so-called 'thee-pillar-model' (Drei-Säulen-Modell) which was introduced by the Ninth Amending Act to the Air Traffic Act[124].[125] The first pillar consists of passenger and luggage checks performed by the aviation authorities.[126] The second pillar is formed by the legal obligations of the airport operators in relation to maintaining safety and security (Eigensicherungspflichten),[127] while the third pillar is constituted by the obligations of the aircraft operators.[128] The enactment of Regulation (EC) No 2320/2002 and its successor has not changed this basic layout. Consequentially, the addressees of the LuftSiG are all airport operators, air carriers and the aviation security authorities.[129]

---

119 *Faust/Lienhart*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 61; see also Bundestag printed paper 15/2361, 2.

120 *Giemulla*, in: Giemulla/van Schyndel 2006, Section 1 'Allgemeines', para. 28.

121 *Giemulla*, in: Giemulla/van Schyndel 2006, § 1 LuftSiG, para. 14.

122 *Giemulla* 2011, 108.

123 The National Aviation Security Programme is marked as classified ('Verschlusssache – nur für den Dienstgebrauch'; security level 4), which means that it is not open to the public. At heart it contains a summary of the German and European provisions. A detailed description is thus impossible, but also unnecessary. The National Aviation Security Programme itself does not have any binding legal effect. Therefore airport and aircraft operators are required to create an aviation security plan of their own. The German Federal Aviation Office (Luftfahr-Bundesamt) performs an evaluation of these security plans and makes directions where necessary in the form of an administrative act which involves a burden and which in turn legally binds its addressee. *Mendel*, in: Giemulla/Rothe 2008, 50.

124 Neuntes Änderungsgesetz zum Luftverkehrsgesetz, BGBl. 1980 I 788.

125 *Richter* 2013, 78.

126 Initially contained in § 29d Air Traffic Act, then in § 29c Air Traffic Act; today in § 5 LuftSiG.

127 Initially contained in § 19b Air Traffic Act, today in § 8 LuftSiG.

128 Initially contained in § 20a Air Traffic Act, today in § 9 LuftSiG.

129 *Richter* 2013, 78.

In the first pillar, the following responsibilities have been established: The national authority responsible for aviation security in terms of Art. 9 of the Civil Aviation Security Regulation is the Federal Ministry of the Interior (Bundesministerium des Inneren, BMI) as the supreme aviation security authority following § 16(4) LuftSiG.[130] Where operational needs are concerned the responsible authority is the Federal Ministry of Transport, Building and Urban Development (Bundesministerium für Verkehr, Bau und Stadtentwicklung, BMVBS) which is also responsible for the Federal Aviation Office.[131] As a result, the BMI is responsible for governmental security measures, while the BMVBS is responsible for cargo screening and security measures that air carriers are obligated to implement.[132] The latter is a result of the fact that the Federal Aviation Office is a subordinate of the BMVBS.[133] The BMI has handed over several of its responsibilities as supreme aviation security authority to the states (Länder) in the context of the instrument of state administration on behalf of the federal government (§ 16(2) LuftSiG).[134] On the whole – when taking into account all 16 state authorities, the Federal Police, the BMI and the BMVBS – there are 20 authorities in Germany that are concerned with aviation security.[135] That means that 'the one' aviation security that is responsible for every aviation security task does not exist.[136]

The LuftSiG consists of 21 paragraphs which are divided into six chapters. In the context of this review chapters 2 and 3 which bear the headings 'Sicherheitsmaßnahmen' (security measures) and 'Unterstützung und Amtshilfe durch die Streitkräfte' (support and administrative assistance by the armed forces). Their most relevant provisions will be presented in the following.

First of all, § 3 LuftSiG contains a sweeping clause (Generalklausel) for the defence of concrete threats. § 3 LuftSiG has to be understood as a catchall clause, especially in relation to § 5 LuftSiG which has been designed as a specific empowerment

130 *Mendel*, in: Giemulla/Rothe 2008, 49.

131 *Faust/Lienhart*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 62; *Richter* 2013, 175 f.

132 *Mendel*, in: Giemulla/Rothe 2008, 49.

133 *Giemulla*, in: Giemulla/van Schyndel 2006, § 2 LuftSiG, para. 5.

134 *Faust/Lienhart*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 63. The consequence of § 16(2) LuftSiG is that the tasks of the aviation security authorities are assumed by the states as a basic principle on behalf of the Bund, unless the Bund claims a task following § 16(3) LuftSiG. *Richter* 2013, 79. The latter is usually the case with larger airports. For example, the local Federal Police Department (Bundespolizeidirektion) is responsible for the enforcement of measures pursuant § 5 LuftSiG at Frankfurt am Main airport, which is Germany's biggest airport, while at the much smaller Zweibrücken airport the Ministerium des Inneren, für Sport und Infrastruktur (Ministry of the Interior, for Sports and Infrastructure) of the state Rheinland-Pfalz is the responsible authority together with the Landesbetrieb Mobilität Rheinland-Pfalz (Management Agency for Mobility). *Richter* 2013, 182, 184.

135 *Mendel*, in: Giemulla/Rothe 2008, 49. For a more detailed description see *Richter* 2013, 173 ff.

136 *Richter* 2013, 79.

(Spezialermächtigung).[137] This is to open up the possibility to react to unforeseen circumstances.[138] The requirement for being able to apply § 3 LuftSiG is the existence of a threat in a particular case ('im Einzelfall bestehende Gefahr'). Where such a threat exists, the aviation security authority can take necessary actions to fend off the threat. The requirements for accepting an incident as such a threat are most likely lower than in the general police law due to the unique abstract endangerment of civil aviation.[139] In practice, § 3 LuftSiG comes into play in order to protect flights or air carriers that have been assessed as being particularly under threat, or in case of concrete warnings that an attack may occur, in order to be able to temporarily implement additional security measures.[140] Being a discretionary power (Ermessensvorschrift),[141] § 3 LuftSiG leaves the choice of the means (the 'How') to the relevant authority, which means that it does not contain any provisions for the concrete use of security measures; the more so as the discretion whether or not to take action (Entschließungsermessen) (the 'If') lies also with the relevant authority.[142] An obligation to act only exists where there is an exclusion of discretionary power (Ermessensreduzierung auf Null).

§ 4 LuftSiG codifies that when discretionary powers must be exercised they have to be based on the principle of proportionality. According to § 4(1) LuftSiG out of several possible and suitable measures the one has to be selected that presumably infringes the affected individual or the general public the least. Following § 4(2) LuftSiG a measure must not result in a detriment which is not proportionate to the intended achievement. Lastly, 3 4(3) LuftSiG rules that a measure is only permissible until its goal has been achieved or until it is revealed that it cannot be achieved. In short, a measure must be possible, suitable, necessary and appropriate. This means that judicial review of the exercise of a discretionary power pursuant § 3 LuftSiG is possible, based on these criteria.[143]

While § 3 LuftSiG provides a way to implement measures in exceptional cases, § 5 LuftSiG contains a catalogue of standard measures that may be introduced by the

---

137 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 67, 69; *Giemulla*, in: Giemulla/van Schyndel 2006, § 3 LuftSiG, para. 1, § 5 LuftSiG, para. 16.

138 *Richter* 2013, 90.

139 *Giemulla*, in: Giemulla/van Schyndel 2006, § 3 LuftSiG, para. 22; cf. VGH Baden-Württemberg, JZ 1983, 102, 106; *Richter* 2013, 91: A measure pursuant § 3 LuftSiG is only permissible where an attack on the security of civil aviation has occurred or where the threat of such an attack is imminent in a particular case. The bar for assessing the likelihood of such an attack must not be set too high. Civil aviation is under constant threat. Thus the likelihood of a threat to civil aviation is sufficient where an attack cannot be ruled out with some certainty.

140 *Richter* 2013, 92.

141 *Giemulla*, in: Giemulla/van Schyndel 2006, § 3 LuftSiG, para. 34.

142 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 68.

143 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 68. Incorrect exercise of a discretionary power would be disuse, misuse and transgression. *Giemulla*, in: Giemulla/van Schyndel 2006, § 3 LuftSiG, para. 37.

aviation security authorities as a specific competence. Thus § 5 LuftSiG, in comparison to § 3 LuftSiG, only requires there to be a general suspicion of a threat which arguably already results from the general vulnerability of civil aviation.[144] Following § 5(1)(1) and (2) LuftSiG, the aviation security authority may search persons who have accessed or want to access those areas of an airport that are not publicly accessible or screen them in another suitable way. It may search, X-ray or screen in another suitable way all objects that have been brought into these areas or are supposed to be brought there. This makes § 5(1) LuftSiG the basis for passenger and luggage screening when entering the airside of the airport.[145] Indications on the concrete design of these security screenings, particularly a list of permissible security measures, can be found in the European legal acts reviewed above. The legislator has chosen the wording 'kann' (can), but since the screenings are demanded by these European legal acts, there is an exclusion of discretionary power.[146] This is an example of how the LuftSiG complements the European provisions by naming addressees – in this case the aviation security authority. § 5(1)(3) LuftSiG allows for the deployment of armed police officers to conduct security screenings, to guard endangered aircraft and to patrol security restricted areas. According to § 5(2) LuftSiG the aviation security authority may ban individuals from non-public parts of an airport if these individuals cannot produce a permit, if they refuse a search or if they refuse to leave behind dangerous objects.[147] § 5(3) LuftSiG is concerned with the screening of hold baggage, cargo, mail[148] and other objects. In order to enforce security measures, the aviation security authority may enter working areas, shops and offices (§ 5(4) LuftSiG).[149] A provision of great significance can be found in § 5(5) LuftSiG. According to § 5(5) LuftSiG the aviation security authority may employ granted contractors (Beliehene)[150] in order to fulfil its obligations resulting from §

144 *Drewes/Malmberg/Walter* 2010, § 4 BPolG, para. 24.

145 However, the powers granted by § 5(1)(1) and (2) LuftSiG are not limited to passengers and their luggage, but also encompass – due to the open wording – all other persons and objects, like employees and cargo. The screening of hold cargo, checked luggage and other objects is again regulated by § 5(3) LuftSiG. If these powers are exercised they amend the obligations of airport operators and air carriers. *Richter* 2013, 93 ff.

146 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 72.

147 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 93; cf. *Giemulla*, in: Giemulla/van Schyndel 2006, § 5 LuftSiG, para. 28 f.

148 Keeping in mind the principle of the confidentiality of the mail (Art. 10 Basic Law) and the provisions of § 5(3)(2) LuftSiG.

149 However, it is not permissible to search these premises on the basis of § 5(4) LuftSiG. *Richter* 2013, 100.

150 Granted contractors are natural or legal persons in the context of civil law that have been granted official authority in order to take over responsibilities of public administration. *Drewes/Malmberg/Walter* 2010, § 4 BPolG, para. 38. They may execute measures in the form of administrative acts as stipulated by § 35(1) of the German Law of Administrative Proceedings (Verwaltungsverfahrensgesetz). *Faust/Lienhart*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 70.

5(1) to (4) LuftSiG.[151] Thus, most of the big airports employ so-called 'aviation security assistants' (Luftsicherheitsassistenten).[152] They are directly bound by the basic rights of the German Basic Law[153] and are usually used in the context of passenger and hand luggage screenings before entering the airside of an airport. Private security companies are contracted to take over these duties; usually subcompanies of the company operating the airport. § 5(6) LuftSiG contains the clarification that the duties and powers of the police remain intact.

Summing up, the main result of § 5 LuftSiG is the conclusion that passenger and hand luggage screenings, the screening of hold luggage and the patrolling of security restricted areas are public responsibilities. Furthermore, the state has the power to conduct further measures, especially to screen cargo and mail, and to ban individuals from the premises. These powers, which stem from § 5(2) and (3) LuftSiG overlap in part with the safeguarding measures of the airport operators (§ 8 LuftSiG) and the air carriers (§ 9 LuftSiG). Where these responsibilities are not taken over by the aviation security authority or by a contractor in its place, they remain legal obligations of the operators. The powers of the aviation security authority then only amend these measures.[154] From the interaction between § 3 and 5 LuftSiG follows that the list of measures according to § 5 is not conclusive; they can be expanded in accordance with § 3.[155] Until 1980 the screenings of passengers and hand luggage were performed solely on the basis of the transport contract (Beförderungsvertrag) between passenger and air carrier.[156] Due to the infringements of the basic rights of passengers inherent to these security procedures, it was decided that public authorities should take over the security checks.[157] This is however somewhat thwarted by the use of granted contractors.

§ 7 LuftSiG is concerned with the conduct of background checks of employees.[158] Background checks were introduced in 1992[159] as a reaction to the Lockerbie

---

151 For a critical review of the use of private parties to maintain security see *Giemulla*, in: Giemulla/Rothe 2008, 36: There are certain core areas where security has to be maintained by the state and not by private parties.

152 Aviation security assistants are persons who have been trained in accordance with the relevant requirements set forth by the BMI, whose personal reliability has been acknowledged as well as their physical and mental suitability. *Richter* 2013, 100 f.

153 *Jarass/Pieroth* 2012, Art. 1 GG, para. 41.

154 *Giemulla*, in: Giemulla/van Schyndel 2006, § 5 LuftSiG, para. 31.

155 Cf. Bundestag printed paper 15/2361, 15.

156 *Giemulla* 2011, 112; *Richter* 2013, 72.

157 Bundestag printed paper 8/3431, 22.

158 For a criticism of the concept of background checks see: *Giemulla*, in: Giemulla/Rothe 2008, 36 f. who claims that background checks promote denunciation.

159 By the Gesetz zur Übertragung der Aufgaben der Bahnpolizei und der Luftsicherheit auf den Bundesgrenzschutz of 23.1.1992, BGBl. 1992 I 178 which introduced a new § 29d into the German Air Traffic Act.

terrorist attack[160].[161] § 7 LuftSiG makes these checks a duty for the aviation security authority. This results from the wording of § 7 LuftSiG and the obligations resulting from Section 11.1 of the Annex of Commission Regulation (EU) No 185/2010. § 7(1) LuftSiG names the categories of employees that have to be checked, which spans from cleaning staff to caterers and pilots.[162] Without a successfully completed background check which leaves no room for doubts on the reliability of the person concerned, that person must not be granted access to restricted areas of the airport or that person must not start his or her job (§ 7(6) LuftSiG). The provisions of § 7 LuftSiG are rendered more precisely by the German Aviation Security Reliability Check Order (LuftSiZÜV, Luftsicherheits-Zuverlässigkeitsüberprüfungsverordnung).[163] § 5(2)(1) LuftSiZÜV stipulates that the results of a background check remain valid for five years; then another check has to be performed. § 7(3)(2) LuftSiG contains provision relating to which agencies may be consulted during the check.[164] A person is deemed reliable where no doubt remains that he or she will fulfil his or her obligations relating to the protection from attacks on the security of civil aviation, especially hi-jacking and sabotage.[165] If doubts remain, a person is classified as unreliable. Thus these provisions burden the person concerned.[166] Which facts may constitute doubts is not conclusively established.[167] Due to the fact that huge amounts of highly sensitive personal data are analysed in the context of a background check, data protection is of the utmost importance. § 6(1) LuftSiG refers to the provisions that govern data handling at the aviation security authorities,[168]

---

160 On 21.12.1988 the PanAm Boeing 747-121 'Clipper Maid of the Sea' exploded above the Scottish town of Lockerbie while on its way from Frankfurt/Main to Detroit. In addition to killing all passengers, persons on the ground were killed by debris falling from the sky. The attack is attributed to Libyan agents. They are said to have smuggled a time-activated bomb into the cargo hold of the aircraft. All in all, 270 persons fall victim to the attack. *Her Majesty's Advocate v Megrahi and Fhimah*, Case No 1475/99.

161 *van Schyndel*, in: Giemulla/van Schyndel 2006, § 7 LuftSiG, para. 2.

162 For a more detailed description see *Hermann*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 105 ff., as well as *van Schyndel*, in: Giemulla/van Schyndel 2006, § 7 LuftSiG, para. 6 ff.

163 BGBl. 2007 I 947.

164 These are the police agencies and the agencies for the protection of the constitution of the states (Länder), the Federal Criminal Police Office, the Federal Office for the Protection of the Constitution, the Federal Intelligence Service, the German Customs Investigation Bureau, the Military Counterintelligence Service and the Federal Commissioner for the Stasi Archives. Additionally the Federal Central Registry (§ 7(3)(3) LuftSiG), the Central Registry of Foreigners and the public authorities responsible for aliens (§ 7(3)(4) LuftSiG), the airport operator, air carriers and the current employer of the person concerned (§ 7(3)(5) LuftSiG). Law enforcement agencies (public prosecution, tax investigation, main customs offices and criminal courts) may also be consulted if the information gathered from inquiries in accordance with § 7(3)(2) and (3) LuftSiG raises suspicions concerning the reliability of the person concerned. *Hermann*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 170 ff., 185.

165 BVerwG, NVwZ 2005, 450, 453; *Hermann*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 196.

166 *Hermann*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 195.

167 *Hermann*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 194 ff.

168 For a list of the relevant provisions for the respective aviation security authority cf. *van Schyndel*, in: Giemulla/van Schyndel 2006, § 6 LuftSiG, para. 10 ff.

whereas § 6(2) LuftSiG establishes an exception: data can be transmitted to other authorities where this is necessary in order to defend against an imminent danger. § 7(11) LuftSiG amends the general provisions for data protection referred to in § 6 LuftSiG with specific rules for the deletion of data.[169]

§ 8 LuftSiG contains provisions for the security measures that have to be implemented by the airport operators and which form the second pillar of the German aviation security concept, as described above. Following § 8(1)(1)(1) LuftSiG the operator is required to design and configure airport facilities, buildings, rooms and accommodations in a way that it enables the necessary constructional and technical protection, the appropriate enforcement of staff security and protection measures and the screening of all non-public areas; furthermore the operator has to provide and maintain the space that is necessary in that context. Exempt from this obligation are devices for the screening of passengers, hand luggage, cargo, mail and hold luggage. Thus the airport operator has to design the airport premises in a way that allows for a realisation of provisions for the use of security measures by laying the constructional foundations.[170] To that end, he has to provide space and rooms.[171] Furthermore, § 8(1)(1)(1) LuftSiG creates an obligation for the airport operator to provide effective physical protection.[172] This can be accomplished for instance through the sufficient lighting of aprons and other parking areas for aircraft, but also by erecting fences and installing access control measures, reinforcing fences with barbed wire, installing bullet-proof glass, etc. Physical protection thus encompasses technical and constructional measures as well as human resources.[173] The obligations are typical examples for so-called 'Eigensicherungspflichten' (legal obligations in relation to maintaining safety and security).[174] Such obligations exist where private companies are required to perform certain actions in the public interest.[175]

§ 8(1)(1)(2) LuftSig is the equivalent to Section 5.2 of the Annex of Regulation (EC) No 300/2008 and Section 5.3 of the Annex of its predecessor, Regulation (EC) No 2320/2002, respectively. It imposes the obligation upon airport operators to transport and store hold luggage, cargo, mail and supplies in a secure way.

---

169 *van Schyndel*, in: Giemulla/van Schyndel 2006, § 7 LuftSiG, para. 71.

170 *Drewes/Malmberg/Walter* 2010, § 4 BPolG, para. 41.

171 This includes the obligation to account for changes in the organization of security measures due to shifts in the security situation. *Richter* 2013, 107.

172 *Faust/Lienhart*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 353.

173 *Faust/Lienhart*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 354.

174 The protection of civil aviation is in the interest of the public as well as in the interest of the airport operators and air carriers. Thus it is permissible to impose upon them obligations in the context of maintaining security and the impositions and restrictions that come with it. *Richter* 2013, 104.

175 *Giemulla*, in: Giemulla/van Schyndel 2006, § 8 LuftSiG, para. 7, 27; *Faust/Lienhart*, in: Hobe/v. Ruckteschell 2009, Vol. 2 A., para. 346; *Giemulla* 2011, 115.

§ 8(1)(1)(4) LuftSiG demands from the airport operator to secure non-public areas of the airport against unauthorised access, and – where sensitive areas are concerned – to allow access only to specifically authorised persons.[176] Sensitive areas are those areas of an airport where terrorist attacks can be directly prepared or executed.[177] This is amended by the obligation to search or screen their own employees, employees of other companies that operate at the airport and other persons in another suitable way before allowing them access to critical parts of security restricted areas (§ 8(1)(1)(5) LuftSiG). This obligation encompasses all objects brought into these areas in order to counter insider threats. This means that one the one hand the access authorisation has to be checked; on the other hand it has to be made sure that no prohibited objects are introduced by employees. These requirements are also considered to be part of the legal obligations of the operator to ensure safety and security. This particular obligations stems from Section 1.3 of the Annex of Regulation (EC) No 300/2008 where it says: 'Persons other than passengers, together with items carried, shall be screened on a continuous random basis upon entering security restricted areas in order to prevent prohibited articles from being introduced into these areas.' In Germany, since January 1st 2006, all employees that work in critical parts of an airport are searched.[178] Until 2005, the workforce of an airport was not screened in any way. Instead, after a successfully completed reliability check, employees could gain access to sensitive areas unchecked; usually through turnstiles unlocked by an ID card.[179] Today, background checks and ID checks are amended by a search.[180] These obligations to search and check employees are however criticised in academic literature. *Giemulla* for instance sees them as an overexpansion of what can be imposed upon an airport operator ('Überdehnung der Eigensicherungspflichten'), since the operators are obliged to go beyond simply supporting public efforts to maintain security by actively having to use security measures of their own.[181]

According to § 8(1)(1)(6) LuftSiG the airport operator is furthermore obligated to train security personnel and also to familiarise other personnel with the task of maintaining security. This is concretised by the Luftsicherheitsschulungsverordnung (Aviation Security Training Order).[182] All security measures of the airport operator

---

176 In practice, identification systems have been proven their value, that go beyond a simple division of airports into a public area and a sensitive area by differentiating between different sensitive areas for instance by using color codes or letter codes. *Richter* 2013, 115.

177 *Faust/Lienhart*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 348.

178 *Mendel*, in: Giemulla/Rothe 2008, 52.

179 *Hermann*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 100.

180 It has to be kept in mind that these security checks have to have the same level as the checks of passengers and their hand luggage, despite the fact that employees are subjected to background checks. *Richter* 2013, 117.

181 *Giemulla* 2011, 115 f.; *Giemulla*, in: Giemulla/van Schyndel 2006, § 8 LuftSiG, para. 7 f., 42 ff.

182 BGBl. 2008 I 647.

have to be depicted in the Aviation Security Plan which has to be presented to the aviation security authority (§ 8(1) LuftSiG).

The obligations of the obligations of the air carriers follow in § 9 LuftSiG the obligations of the airport operators. These obligations bind any carrier that operates aircraft that weigh more than 5,7 t[183], as long as it is a German carrier, even if that carrier operates abroad, as well as foreign carriers that operate at German airports (§ 9(2) LuftSiG). The obligations are similar to those of the airport operators and partially have identical wording. For instance, § 9(1)(1)(3) LuftSiG similarly to § 8(1)(1)(6) LuftSiG requires training of employees in matters of aviation security. One of the main aspects of the obligations of air carriers is securing the aircraft they operate and the areas of the airport allocated to them against unauthorised access. In the case of securing aircraft, this can occur in the form of human guards or by technical means, for instance by removing stairs, boarding bridges or ramps, locking all doors and using security bolts.[184] The choice of a specific measure is left to the air carriers. This is also the case in the context of securing areas of the airport allocated to them. Another main aspect is the obligation to relate luggage to the respective passenger, which results from § 9(1)(1)(1) LuftSiG which demands that security measures must be taken in the context of processing passengers, luggage, cargo, mail and supplies. The obligation to relate luggage to passengers as a security measure goes back to scenarios where terrorists gave up luggage containing explosive devices, but did not board the plane, detonating the explosive device from the ground or with a timer.[185] The measure thus serves the identification of unaccompanied pieces of luggage. However, in contrast to past provisions, it is generally permissible to transport such pieces of luggage if they were subjected to proper screening. This is owed to the fact that modern security measures, especially advanced X-ray devices and explosive detection systems, make it less and less likely that dangerous objects can be introduced as hold luggage.[186] Furthermore an obligation to check flight tickets and boarding passes results from § 9(1)(1)(1) LuftSiG, as well as an obligation to screen cargo and mail. This is the third focal point of air carrier obligations. The obligation to screen cargo does not apply when the cargo has already been screened by a 'regulated agent' or where the consignor is a

183 However, according to § 9(4) LuftSiG, owners of other aircraft may also be bound if this is necessary to maintain security.

184 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 371.

185 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 375. This was probably how the Lockerbie terrorist attack in 1988 was executed. However, the details of that event remain unexplained even today. *Meikle, J./Carrell, S.*, Mystery of Lockerbie plane bombing may never be solved, The Guardian, Main Section, 21.5.2012, 2.

186 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 375.

so-called 'known consignor'.[187] This means that cargo screening does not necessarily have to occur at the airport. The obligations of air carriers resulting from § 9(1)(1)(1) LuftSiG only apply, where they are not taken over by the aviation security authority.[188]

§ 11(1) LuftSiG contains a list of prohibited items that must not be carried in hand luggage or on a person. A prohibited item in the context of § 11(1) LuftSiG is an item that can be used for an unlawful intervention.[189] In principle, this list is identical with and even refers to the list that can be found in Annex 4-C of Commission Regulation (EU) No 185/2010. According to § 11(2) LuftSiG, exceptions from the bans listed in § 11(1) are possible where this is a necessity and a permit can be presented if such a permit is required according to other statutory provisions. This has been utilised to make it possible for employees working in restricted areas to introduce items that are prohibited, but required in the context of their work.[190] § 19 LuftSiG makes carrying prohibited items into aircrafts or in restricted parts of airports a punishable offence. The attempt to introduce such an item is however not punishable. If such an attempt is discovered, the item is confiscated, but it was decided not to unnecessarily criminalise passengers.[191]

§ 12 LuftSiG contains the powers of the pilot in command.[192] During flight, he has to maintain security and order on board as a granted contractor. To this end he is granted the power to determine the identity of a person, to seize items, to search persons and items and to restrain a person (§ 12(2) LuftSiG). Physical violence may only be used by him or his agents as a last resort. These powers only apply if the aircraft travels through German or stateless airspace.[193]

---

187 Further exemptions result from Section 6.1(1) of the Annex of Regulation (EC) No 300/2008 and Section 6.1.1 of the Annex of Commission Regulation (EU) No 185/2010, for instance where transfer cargo is transported.

188 Cf. *Richter* 2013, 130 f. Passenger and luggage screening only have to be conducted by an air carrier, where governmental security checks are not available, for instance when a big aircraft takes off at an airport where there are no governmental security checks. Bundestag printed paper 15/2361, 19.

189 *van Schyndel*, in: Giemulla/van Schyndel 2006, § 11 LuftSiG, para. 13.

190 *Faust/Leininger*, in: Hobe/v. Ruckteschell 2009, Vol. 2, Part 2 A., para. 75.

191 *Richter* 2013, 89.

192 The pilot in command is appointed by the respective air carrier: see § 41(1) of the Betriebsordnung für Luftfahrtgeräte of March 4th 1970 (Plant Regulations Governing the Operation of Aircraft), BGBl. 1970 I 262.

193 *Drewes/Malmberg/Walter* 2010, § 4a BPolG, para. 42. This results from the fact, that aircraft are not part of their homeland's territory: they do not constitute extraterritorial zones (territoriality principle). Thus when determining which law has to be applied, the current location of an aircraft is the decisive factor. If an aircraft travels through the airspace of a foreign country, the law of that country applies. Art. 1 of the Chicago Convention stipulates that any signatory state has full sovereignty over his airspace. *Richter* 2013, 159; cf. *Drewes/Malmberg/Walter* 2010, § 4a BPolG, para. 21. The application of the law of the home country of an aircraft results from the so-called flag law principle (Flaggenrechtsprinzip), whereby a subsidiary continued applicability

As the last part, § 14(3) LuftSiG shall be presented, which was nullified by the German Federal Constitutional Court (Bundesverfassungsgericht).[194] § 13, 14 and 15 of the LuftSiG govern cases in which the German military (Bundeswehr) may act in the context of aviation security. In particular, the Bundeswehr is permitted to force aircraft off course or to land, to threaten the use of armed force and to fire warning shots in order to prevent an especially serious disaster from occurring (§ 14(1) LuftSiG). Such order to such measures may be given by the Minster of Defence, or the head of the German Air Force (Inspekteur der Luftwaffe) if empowered to do so by the minister. Is has been pointed out above, that the enactment of the LuftSiG was a reaction to the events of 2001 and 2003. In order to counter scenarios like these, § 14(3) LuftSiG contained provisions that would have empowered the Minster of Defence to use armed force to shoot down an aircraft, if following an evaluation of the circumstances it has to be expected that the aircraft will be used against human lives and if such an action is the only measure available to counter that threat; thus amending the measures available to the Bundeswehr. Shooting down a hijacked aircraft which is about to be used as a weapon can be understood as a reactive security measure which comes into play while a terrorist attack is occurring. Such a scenario is called a 'renegade case'.[195]

The judgement of the Bundesverfassungsgericht relating to § 14(3) LuftSiG ruled that shooting down a passenger plane is irreconcilable with the dignity of man and the right to life where innocent bystanders aboard are affected.[196] Human beings would become mere objects of a rescue operation to save others. Such a treatment disregards them as subjects with dignity and unalienable rights. Since their deaths are the means to save others, they are reified and disfranchised. Their lives are commanded by the state and these people who themselves are the victims of a

---

of that law is carried out. *Richter* 2013, 166. However, measures performed or ordered by the pilot in command can be executed on the basis of the Tokyo Convention (Convention on Offences and Certain Other Acts Committed On Board Aircraft of September 14th 1963). In such a case, according to Art. 10 of the Tokyo Convention a person cannot be held to account if acting in accordance with the Convention. Furthermore, private law powers in relation to the passengers result from the transport contract. *Richter* 2013, 165 f. Emergency powers (e.g. self-defence) may also serve as a basis for performing certain measures. According to § 4 of the German Criminal Code (Strafgesetzbuch, StGB), German law applies to criminal acts performed aboard German aircraft.

194 BVerfGE 115, 118, 139.

195 *Richter* 2013, 73. For a description of the legal situation in other countries see *Giemulla/Rothe*, in: Giemulla/Rothe 2008, 97 ff.: In the USA and Canada there is no legal norm that permits shooting down civil aircraft. Nevertheless, the US-president is said to have such power which results from his status as commander-in-chief of the armed forces. In Canada, the power is derived from the royal prerogative. In France, however, such a legal norm exists: the Décret no. 75-930 du 10 octobre 1975 relatif à la défense aérienne empowers the commander of the aerial defence to give the order to shoot down an aircraft. In the Netherlands, Austria, Norway, Poland, Russia and Slovakia a similar power is based on diverse legal foundations. However, only Poland, Russia and Slovakia have created similar norms as France.

196 BVerfGE 115, 118, 139 f., 151 ff. Cf. *Giemulla* 2011, 119 ff.

hijacking in need of protection are thus stripped of the value and dignity inherent to all human beings.[197] The Bundeswehr may in fact be used in the interior in accordance with Art. 35(2)(2) Basic Law if so requested by a state (Land) and if this is necessary in order to prevent a severe disaster, which includes a situation where an aircraft is going to be used against the lives of human beings.[198] However, no military grade weapons, for instance the weapons of a fighter jet as would be required by § 14(3) LuftSiG, may be used, but only weapons that the law of the state requesting assistance has deemed appropriate for police use.[199]

Following an abstract judicial review request (abstrakte Normenkontrolle)[200] by the states (Länder) Hessen and Bayern, the court clarified in a plenum decision (Plenarbeschluss)[201] that the use of military weapons at home is possible as a last resort and in fact not entirely barred by Art. 35(2)(2) and (3) of the Basic Law. However, it is not sufficient that the police are over-burdened.[202] The Bundeswehr may only use military weapons at home where this is rendered necessary by an especially severe disaster.[203] Even where speed is essential, the federal government as a collegiate body has to greenlight the deployment.[204] A deployment of the air force to shoot down passenger aircraft that are used as weapons remains impermissible, however. This might be different, where there are no innocents aboard an aircraft, just the attackers. In such a case, shooting down the aircraft might be allowed as long as the requirements set forth by the court are fulfilled.[205]

In summary, it can be said that the LuftSiG is vague when it comes to setting out requirements for how to use security measures in civil aviation. It does however contain detailed requirements on where, if and by whom security measures are used by connecting the addressless provisions of European civil aviation security law to specific addressees.

---

197 BVerfGE 115, 118, 154.

198 BVerfGE 115, 118, 148 f.

199 BVerfGE 115, 118, 146 f. See also *Binninger*, in: Giemulla/Rothe 2008, 23.

200 The review originally referred to § 13 to 15 LuftSiG, but the applicants reduced their request to § 13, § 14(1), (2) and (4) and § 15 LuftSiG after the court had declared § 14(3) LuftSiG invalid. Cf. BVerfG, 2 PBvU 1/11 vom 3.7.2012, para. 5.

201 BVerfG, 2 PBvU 1/11 of 3.7.2012, NVwZ 2012, 1239.

202 BVerfG, 2 PBvU 1/11 of 3.7.2012, para. 26.

203 BVerfG, 2 PBvU 1/11 of 3.7.2012, para. 42 ff.

204 BVerfG, 2 PBvU 1/11 of 3.7.2012, para. 53.

205 *Murswiek*, in: Sachs 2011, Art. 2 GG, para. 182a; critical: *Kutscha*, in: Roggan/Kutscha 2006, 44 f.: The question is, what the requirements are for being able to assess with necessary certainty that an aircraft is manned solely by terrorists and is about to be used as a weapon. And how can be excluded that innocent people are killed by debris when the aircraft is shot down? On the topic of the consequences of a passenger aircraft hitting the ground see *Freitas*, Journal of Transportation Security 2/2012, 107, 107 ff.

3.4 Aviation security regulation in the United Kingdom

The British provisions are quite similar to those applied in Germany. This is not surprising, since they are all based on European aviation security law. This chapter will thus only review those specific characteristics of British aviation security law that distinguish it from German aviation security law. First of all, it has to be pointed out that the United Kingdom has often played a leading role in the continuing revolution of aviation security. Examples for this can be found in the field of cargo screening and in the introduction of security screening for airline and airport personnel.

The central authority responsible for security in all forms of public transport is the Department for Transport (DfT). The DfT is the supreme authority in all matters relating to security in civil aviation, maritime transportation, national railways, London Underground and the Eurotunnel[206]. Directly responsible for the security of airports is usually the local Chief Constable.[207] This was at first governed through a 'designation' of individual airports by the Secretary of State for Transport following s25(1) Aviation Security Act 1982[208], which has since been repealed.[209] This system was replaced with a new one by s80 in conjunction with Schedule 6 of the Policing and Crime Act 2009[210].[211] Following the new system, all airports that are the addressees of a Direction according to s12, 13 or 14 of the Aviation Security Act 1982 (so-called 'relevant aerodromes') are obligated to form a Police Service Agreement with the local police, if the security plan of the airport stipulates the dedication of police officers to secure the airport (s25B(1) Aviation Security Act 1982). This security plan is established by the Security Executive Group of the airport, which follows recommendations made by the Risk Advisory Group of the airport[212].[213] Any airport

206 In cooperation with the French authorities.

207 In the United Kingdom, the regular police forces (called 'Territorial Police Forces'; in contrast to special police forces like the British Transport Police) are divided by regions. For instance the Metropolitan Police Service is responsible for the region Greater London, not including the City of London; the Leicestershire Police is responsible for the regions Leicestershire, Leicester and Rutland. The Chief Constable is the leader of such a territorial police force (except with the Metropolitan Police and the City of London Police).

208 c. 36.

209 The airports that were designated according to s25(1) Aviation Security Act 1982 were London Heathrow, London Gatwick, London Stansted, Aberdeen, Edinburgh, Glasgow International, Glasgow Prestwick, Birmingham and Manchester.

210 c. 26.

211 *Walker* 2011, para. 10.120.

212 Here, a method called 'Multi-Agency Threat and Risk Assessment is used. The method was introduced following recommendations of the so-called *Wheeler* report: Department for Transport 2002. Its goal is to increase cooperation between those actors at the airport that are concerned with different aspects of airport security.

213 For a detailed description of the planning cycle see Department for Transport 2010, 4: The Risk Advisory Group drafts a Risk Report which in turn is accepted or amended by the Security Executive Group. In the end, the Security Executive Group creates the Airport Security Plan based on the analysis provided by the Risk Advisory Group.

operator has to install these groups (s24AB(1) and s24AG(1) Aviation Security Act 1982). The Risk Advisory Group creates a risk analysis of the terrorist threat and other threats to the airport, while the Security Executive Group makes decisions against or in favour of introducing certain security measures based on this analysis.[214] Local police are represented in both groups following s24AB(2)(b) and s24AG(2)(b), (c) Aviation Security Act 1982. If a decision is made in favour of a dedicated police presence at the airport – as is usually the case – a Police Service Agreement is set up between the airport operator and the local police force.[215] Following s26(1) Aviation Security Act 1982, members of this police presence are authorized to access any part of the airport even without consent of the operator. Furthermore, the airport operator has to bear the cost of the police presence and provide accommodation (s26(3) Aviation Security Act 1982). All costs are pre-determined by the Police Service Agreement.

The core of aviation security law in Great Britain is the aforementioned Aviation Security Act 1982, which came into force on October 23 1982. The act contains in sections 12(1) and (6), 13(1) and (2)(c), 13A(1), 14(1A), (2) and (3), 15(1) and (4), 17(1) and 38(6) a number of arrangements that give the Secretary of State for Transport the competence to make Directions concerning the use of security measures[216].[217] The scope of the Directions is limited to aviation security by the recurring phrase 'for purposes to which this Part of this Act applies. Addressees of such Directions are mainly airport operators, but also air carriers and persons who use parts of the airport grounds or who offer services in areas of the airport with restricted access, meaning that Directions can also be addressed to caterers and other suppliers. For instance s12(1)(a) Aviation Security Act 1982 stipulates: '[…]the Secretary of State may give a direction in writing to the operator of any one or more aircraft registered or operating in the United Kingdom, or to the manager of any aerodrome in the United Kingdom, requiring him not to cause or permit persons or property to go or be taken on board any aircraft to which the direction relates, or to come or be brought into proximity to any such aircraft, unless such searches of those persons or that property as are specified in the direction have been carried out by constables or by other persons of a description specified in the direction.'

---

214 Cf. *Walker* 2011, para. 10.115.

215 National Policing Improvement Agency 2011, 12.

216 Furthermore, following s21F(1) Aviation Security Act 1982 the Secretary may enact provision relating to aviation cargo security in the form of Regulations. These can be found in the Aviation Security (Air Cargo Agents) Regulations 1993 (SI 1993/1073). *Walker* 2011, para. 10.118.

217 Following the enactment of the Civil Aviation Act 2012 (c. 19), compliance with these Directions is upheld by the Civil Aviation Authority. The Civil Aviation Authority also provides advice to the Secretary of State for Transport.

One example for such a Direction of the Security Scanners (Heathrow Airport) (No. 3) Direction 2011.[218] In this Direction the Head of Division of the Aviation Security Division of the DfT, acting on behalf of the Secretary of State for Transport, directs the operator of the country's biggest airport, London Heathrow, to use security scanners for passenger screening. Use of the scanners must occur in accordance with the provisions of the Code of Practice for the Acceptable Use of Security Scanners in an Aviation Security Environment, enacted in November 2011. This code of practice is basically a written out version of the provisions of Commission Regulation (EU) No 185/2010 concerning the use of body scanners. Beyond that, an airport operator has to check twice a year that no scan images can be saved, copied or sent. Both the use of image analysis software ('automatic threat recognition software') and manual evaluation of the images are allowed. The use of security scanners must be announced to passengers using the following wording: 'For the benefit of all passengers' security, passengers may be required to be screened using security scanning equipment. Screening will be conducted by security screeners acting on behalf of the airport operator. Images of passengers will not be saved.'[219] The devices may only be operated by trained personnel. The most significant deviation from the provisions of Commission Regulation (EU) No 185/2010 can be summarized under the motto 'no scan – no fly'.[220] This means that passengers cannot choose an alternative screening method. There is no 'opt out'; passengers have to endure being subjected to the scanners. The reasoning behind this is the conviction that a manual screening is not equal to a screening using a security scanner.[221] The 'no scan – no fly' principle is currently under scrutiny.[222] Another thing that has to be pointed out is the fact that children are not exempt from being screened by the scanners. An Operational Protocol[223], which is not available to the public, contains further provisions about the use of security scanners, among others concerning the process of selecting passengers for screening. Despite the fact that the introduction of body scanners at British airports was indeed accompanied by protests, the House of Commons Home Affairs Committee succinctly stated: 'Air passengers already tolerate a large invasion of their privacy and we do not feel that full body scanner

---

218 Direction (No. 3) to the airport operator of Heathrow airport under the Aviation Security Act 1982 relating to security scanners 2011 of 5.12.2011.

219 Department for Transport 2011a, 4.

220 'If a passenger declines to be scanned that passenger must be refused access to the restricted area of the airport (the Critical Part), with the result that the passenger will not be able to fly on that occasion.' Department for Transport 2011a, 5.

221 'I do not believe that a 'pat down' search is equivalent in security terms to a security scan.' Secretary of State for Transport *Justine Greening*: House of Commons, Daily Hansard, Written Ministerial Statements, 21.11.2011, Col. 15WS.

222 *R (on the application of Sarwar) v Secretary of State for Transport*, on-going.

223 Contained in Annex D of the Security Scanners (Heathrow Airport) (No. 3) Direction 2011.

add greatly to this situation.'[224] Concerns about infringements of privacy caused by the scanners were described as being overstated.

The pattern described above is typical of British security legislation in the field of public transport security. Acts of Parliament do not contain concrete provisions, but merely authorize the relevant Secretary to enact such provisions in the form of Directions or Regulations. These often refer to a certain Code of Practice.

All 'more stringent measures' according to Art. 6 of Regulation (EC) No 300/2008 are collected in the Single Consolidated Direction (Aviation) 2010, which is part of the National Aviation Security Programme. Both documents are classified and thus cannot be reviewed here. Additionally, the operators of individual airports may implement further more stringent measures. The result is that security measures and processes may differ from airport to airport. For instance, one airport may ask passengers to remove their belts before screening, while another airport does not.

From the provisions of the Equality Act 2010 result requirements for the handling of disabled passengers and for the protection of their rights, especially the right to have access to certain facilities that are part of public life which includes public transport. This aspect is represented in concentrated form in a Code of Practice which is concerned with access of disabled persons to air travel.[225] The Code recommends establishing private areas for physical screenings of disabled persons[226] and reminds special care when handling disabled passengers. However, disabled persons are not at all excluded from security screenings.[227] Furthermore, the Equality Act 2010 contains provisions concerning the use of profiling and the selection of passengers for screening. The selection process must not be based on age, disability, gender reassignment, marriage and civil partnership, race, religion or belief, sex or sexual orientation.[228]

British aviation security law is currently in a process of restructuring, deregulation and modernization. Where to date the different actors in civil aviation are addressed with certain provisions, that system is to be replaced by a more flexible one. Keywords are 'outcome focused', 'risk based' and 'direct and inspect'. 'This will provide the industry with more freedom to deliver bespoke solutions, focused on achieving security outcomes rather than having to follow prescriptive measures.'[229] At the same time it is clarified that: 'Government will always retain its ultimate

224 House of Commons 2010, HC 311, 12.

225 Department for Transport 2008, especially 56 f.

226 Department for Transport 2008, para. 5.31: 'A private area should be available on request for physical searches or where a passenger has personal medical equipment which they do not wish to expose in public.'

227 Cf. the provisions of ECAC Doc. 30 Part I Annex 5B-2.

228 Cf. Part 2 Chapter 1 of the Equality Act 2010.

229 Department for Transport 2011, 1.4. Cf. 2.3 and 2.4 of the report.

responsibility for aviation security, continue to establish the threat and risk picture, and specific security outcomes for the industry to meet.'[230] The bottom line is that in the future, the state will limit its role to stipulating security objectives that have to be achieved (for instance 100% cargo screening). How these objectives are achieved is left to the relevant actors – keeping in mind the provision contained in European aviation security law. However, the authority of the Secretary of State for Transport to make Directions based on the Aviation Security Act 1982 will remain intact. The introduction of the new system is broken down into several phases and is expected to be completed in 2016. Progress, however, seems to be slow.[231]

3.5 Summary and Outlook

Whereas German law stipulates that security checks of passengers between the landside and the airside of an airport are a sovereign task (while maintaining the possibility to delegate this task to granted contractors), the same task is executed by the aviation industry in the United Kingdom (however under the supervision of the Department for Transport).

All in all, it has to be asserted that the British approach is more flexible than the German approach. This flexibility – which will be expanded in the coming years – however comes at the price of a heterogeneous implementation of SMTs. The planned deregulation will increase that flexibility. It is all the more important that passengers are thoroughly informed about SMTs in order to be able to adapt to the SMTs implemented at the airport of their choice. Deregulation is limited by the provisions of European law, which are meant to lead to a harmonization within the European Union. However, the possibility to implement more stringent measures means that there is a method to weaken this harmonization.

Civil aviation is an international phenomenon. Especially traveling within the European Union has become more attractive than ever thanks to the provisions of the Schengen Agreement, the introduction of a common European currency and cheap plane tickets. But this internationality also brings with it severe issues. For an SMT design that respects human rights in a passenger's country of origin will be of little value where the opposite is the case at the passenger's destination. This underlines the importance of harmonizing aviation security not just within the European Union, but worldwide. The rules set forth by the ICAO can be seen as an important step in the right direction in this regard. The European provisions specify them and limit differences in aviation security.

---

230 Department for Transport 2011, 1.5.

231 House of Commons 2013, HC 78-II, Ev 238, para. 20.

3.6 Possibilities for circumvention

The review of legislation concerned with aviation security at European level and in the Federal Republic of Germany and the United Kingdom has revealed that the law governing the use of SMTs is quite dense. White lists dictate which types of SMTs may be used, thus excluding every type of SMT that is not listed. However, detailed modalities of how exactly an SMT listed has to be operated are rarely given. This means that operators may choose different design options that may or may not result in the infringement of basic rights.

Furthermore, opportunities to circumvent these provisions remain. Deviations from European requirements are possible as long as the minimum standards for security that have been established are maintained. These deviations come in the form of 'more stringent measures'. However, it is hardly possible to qualify this as a 'lack' of legislation. Rather, the possibility to implement more stringent measures is a purposefully installed political tool to allow member states of the European Union to go beyond the European standards if so intended.

The main issue with this concept is that a more stringent measure may lead to infringements of passenger rights. For instance the 'no scan no fly' policy adopted in the United Kingdom for the use of body scanners means that passengers are stripped off their right to opt for an alternative screening method. While – arguably – increasing security, this more stringent measure comes at the price of a decrease in personal liberty.

New SMTs for screening may be introduced as more stringent measures, but also in the context of field tests following 12.8.1(a) of Commission Regulation (EU) No 185/2010. The duration of a testing period is limited. However, this can still be seen as a gateway for screening technologies that are more intrusive than the standard measures predetermined by European law.

3.7 Excursion: Security in rail transportation

In order to broaden the view, this chapter will look briefly at the legal provisions regarding the implementation of security measures in public rail transportation.

At the international and European level, legal provisions that are directly concerned with the use of security measures in rail transportation, comparable to the regulations that regulate the use of security measures in the field of aviation security, do not exist. However, there are legal provisions which indirectly affect the use of security measures, most prominently the European Data Protection Directive. Furthermore, the basic rights recognized by the member states of the European

Union set a framework for the use of security measures. The European Union has indicated in a working paper[232] that a concrete legal framework for the use of security measures in rail transport may be created at some point in the future; however, reactions to this advance have been mainly negative.[233]

In Germany, the situation is similar. Relevant acts like the Allgemeine Eisenbahngesetz[234], the Eisenbahn-Bau- und Betriebsordnung[235] and the Verordnung über den Bau und Betrieb der Straßenbahnen[236] use the word 'Sicherheit', which corresponds to both 'security' and 'safety' in the English language, but the meaning of the term is in this context limited to 'safety'. However, the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG)[237] and the acts containing the legal framework regulating the work of the police forces of the individual German states and the federal police forces, particularly the German Federal Police, which – among other responsibilities – is tasked with policing the infrastructure of Deutsche Bahn, do regulate the use of CCTV. Provisions comparable to those that regulate the use of security measures in aviation security do not exist.

In the United Kingdom, the central norm when it comes to rail security is s119(1) of the Railways Act 1993. This section allows the Secretary of State for Transport to give directions to railway operators concerning the protection of people and property, i.e. the use of security measures. These directions are collected in the National Railway Security Programme, which is not accessible to the public. This means, that railway security follows a similar scheme as aviation security in the United Kingdom. A Code of Practice[238] contains provisions for train station design with regard to the special needs of disabled persons. More general provisions for the design of stations, particularly for the minimization of the effects of explosions, can be found in the 'Security in Design of Stations Guide'.[239] The British Transport Police is tasked with policing the railways. The use of personal data and CCTV is regulated by the Data Protection Act 1998[240], the CCTV Code of Practice and the Code of Practice for Surveillance Camera Systems (pursuant to s29 of the Protection of Freedoms Act 2012).

---

232 Commission Staff Working Document on Transport Security, 31 May 2012, SWD(2012) 143 final.

233 Cf. House of Commons 2013, HC 875, 3, 18: 'There was a distinct lack of enthusiasm, both from Government and industry, for further EU involvement in relation to land transport security, not least because the Government was concerned that action at EU-level might result in the levelling down of existing security measures in the UK. '.

234 BGBl. 1993 I 2378, 2396; 1994 I 2439.

235 BGBl. 1967 II 1563.

236 BGBl. 1987 I 2648.

237 BGBl. 2003 I 66.

238 Department for Transport 2011b.

239 Department for Transport 2012, para. 3.1 ff.

240 c. 29.

All things considered, the main distinction between rail transport security in Germany and in the United Kingdom is a more extensive use of CCTV in the United Kingdom. However, both countries heavily rely on CCTV when it comes to maintaining security in rail transportation.

4. Level of protection of affected groups

The main categories of people who come into contact with SMTs in public transport are passengers and employees, which can then be further subdivided into groups and sorted by gender, age etc. A comprehensive summary and description of such groups in the context of the SIAM case studies can be found in D4.1 of the SIAM project.

4.1 Passengers

In work package 4 of the SIAM project, the following attributes have been defined to differentiate between passenger groups:

- gender
- age
- purpose of travel
- nationality
- race
- religion
- disability

This list is not conclusive. Further attributes could be identified. However, the abovementioned attributes have been carved out as being the most relevant attributes in the context of mass transportation security in work package 4 of the SIAM project.

4.1.1 Discrimination of passengers

Discrimination of individuals and groups of persons is prohibited by a number of legal acts. The following are examples of explicit bans of discrimination found at international, European and national level:

- Art. 26 of the International Covenant on Civil and Political Rights: 'All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.'

- Art. 14 of the European Convention on Human Rights:[241] 'The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.'

- Art. 1(1) of Protocol No. 12 to the European Convention on Human Rights: 'The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.'

- Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin

- Art. 21 of the Charter of Fundamental Rights of the European Union: 'Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.'

- Art. 3(3) of the German Basic Law (Grundgesetz): 'No person shall be favoured or disfavoured because of sex, parentage, race, language, homeland and origin, faith, or religious or political opinions. No person shall be disfavoured because of disability.'

- The Equality Act 2010 (c.15) in the United Kingdom

Individual groups of passengers are not exempt from individual security measures. An example of this can be found on page 2 of Annex 5B of Part I of ECAC Document No. 30 where it says that '[d]isabled persons and persons with reduced mobility (PRMs) are not exempt from security checks, but it is important that such checks are carried out carefully and sensitively.'

[241] Full title: Convention for the Protection of Human Rights and Fundamental Freedoms.

4.1.2 Freedoms of passenger groups

In practice, certain SMTs may still affect certain groups of people more than others. A person who wears religious clothing to cover the body may be more affected by the use of a body scanner than others. A person who carries a medical device on his or her body that contains metal components will be more affected by the use of metal detectors than others. As a basic principle, a female passenger will be more affected by a pat-down by a male security officer than a male passenger and vice versa. These are just some examples of how certain SMTs affect certain groups of people in a different way.

The following tables will map selected SMTs with freedom infringements related to certain groups of passengers in order to demonstrate the differences between the impacts of the SMTs on these groups, thus amending the data collected in deliverable 4.2 of the SIAM project. This will give a basic indication of the level of protection of certain passenger groups resulting from the use of certain types of SMTs.

Body scanners

Passenger groups relating to certain attributes	**Security practices and situations**	**Related freedoms**[242]
Gender	*presenting images to security personnel:* women will be significantly more affected than men where images created by a scanner are displayed to male security personnel (voyeurism); where images are displayed, men may be ridiculed by security personnel (e.g. for having small genitalia); both men and women are equally in danger of being ridiculed by security personnel because of the shape of their body (e.g. being overweight, having bad posture); transgender persons will also be significantly affected where images are shown to security personnel	presumption of innocence, equal treatment and non-discrimination, privacy and data protection

[242] As identified in deliverable 4.2 of the SIAM project.

Age	*creating images of the human body:* where small children are sent through a scanner, this may violate child pornography laws; senior citizens may be unfamiliar with body scanners and thus overwhelmed or overstrained by them	presumption of innocence, equal treatment and non-discrimination, privacy and data protection
Purpose of travel	*emitting radiation:* frequent flyers will be more affected by any radiation emitted by the scanners due to the dangers of an accumulative effect of the radiation; persons who are forced to use a certain mode of transportation (e.g. persons travelling by command of their employer, deportees, detainees) resulting in the compulsion to undergo a certain security measure are more affected than persons who do have a choice whether to travel or not	bodily integrity, presumption of innocence, equal treatment and non-discrimination, privacy and data protection
Nationality	*creating images of the human body:* members of certain ethnic groups may be more affected by the scanning of the human body than others due to cultural conceptions	presumption of innocence, equal treatment and non-discrimination, privacy and data protection
Race	-	-
Religion	*creating images of the human body:* members of certain religions / religious groups may be more affected by the scanning of the human body than others because they feel that this is inconsistent with their religious beliefs	presumption of innocence, equal treatment and non-discrimination, privacy and data protection
Disability	*requiring passengers to stand up during scans:* persons with disabilities may not be able to stand up for a scan (e.g. because they are confined to a wheelchair); *scanning the human body for prohibited articles:* medical aids, prostheses etc. may be mistaken for prohibited articles; *being confined to the scanner for the duration of the scan and having to stand still:* persons	freedom of movement, presumption of innocence, equal treatment and non-discrimination, privacy and data protection

	with mental disorders may be frightened by the procedure	
Other	-	-

Smart CCTV

Passenger groups relating to certain attributes	**Security practices and situations**	**Related freedoms**
Gender	*having facial recognition as part of the CCTV system:* beards may affect recognition performance; *storing images and/or displaying them to security personnel:* women may be targeted by male security personnel in the context of voyeurism and vice versa; *having profiling as part of the CCTV system:* see below under the heading 'Passenger profiling'	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Age	*having facial recognition as part of the CCTV system:* age may affect recognition performance; *having behaviour recognition as part of the CCTV system:* the behaviour of children may be misinterpreted as suspicious or dangerous behaviour; *having profiling as part of the CCTV system:* see below under the heading 'Passenger profiling'	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Purpose of travel	*having profiling as part of the CCTV system:* see below under the heading 'Passenger profiling'	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Nationality	*having behaviour recognition as part of the CCTV system:* foreigners may exhibit innocuous behaviour that is misinterpreted as suspicious or	presumption of innocence, equal treatment and non-discrimination, privacy and data protection,

	dangerous by the system	freedom of movement
Race	*having profiling as part of the CCTV system:* see below under the heading 'Passenger profiling'	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Religion	*having behaviour recognition as part of the CCTV system:* members of certain religions may exhibit behaviour that is misinterpreted as suspicious or dangerous by the system; *having profiling as part of the CCTV system:* see below under the heading 'Passenger profiling'	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Disability	*having behaviour recognition as part of the CCTV system:* the behaviour of persons with mental disorders may be misinterpreted as suspicious or dangerous ; the same may be true for certain physical disorders (e.g. walking disabilities)	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Other[243]	*having behaviour recognition as part of the CCTV system:* the behaviour of certain social groups may be considered dangerous, suspicious or simply 'undesirable' by the system	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement

Biometrics

Passenger groups relating to certain attributes	**Security practices and situations**	**Related freedoms**
Gender	-	-
Age	*relying on a specific biometric feature for recognition:* age may affect the	presumption of innocence, equal

[243] This category has been included as a catch-all element.

	recognition of certain biometric features	treatment and non-discrimination, privacy and data protection, freedom of movement
Purpose of travel	*making registration mandatory:* business travellers and other frequent flyers may already be enrolled in the system while other passengers may not, thus prolonging the overall procedure; persons who are forced to use a certain mode of transportation (e.g. persons travelling by command of their employer, deportees, detainees) resulting in the compulsion to undergo a certain security measure are more affected than persons who do have a choice whether or not to travel	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Nationality	-	-
Race	*relying on a specific biometric feature for recognition:* members of certain racial groups may differ in the characteristics of certain biometric features (e.g. the system may be better at recognizing Asian passengers than it is at recognizing African passengers)	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Religion	*relying on a specific biometric feature for recognition:* certain religious groups may object to the use of certain biometric features for recognition	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Disability	*relying on a specific biometric feature for recognition:* certain disabilities may make biometric recognition impossible	presumption of innocence, equal treatment and non-discrimination, privacy and data protection, freedom of movement
Other	*relying on a specific biometric feature for recognition:* a person may not possess the biometric features	presumption of innocence, equal treatment and non-

	required for recognition due to abrasion, disease, disability, amputation, etc.; or the feature may have been stolen and misused by others so that this feature is now blocked / disabled	discrimination, privacy and data protection, freedom of movement

Another issue lies with the use of profiling as it is the one SMT that is designed for the active selection of passengers for further screening based on certain attributes. It is thus a precursor to additional measures. Profiling can be defined as performing an evaluation of a person based on certain predetermined criteria.[244] Profiling can be based on a person's behaviour, appearance and a multitude of other personal attributes. Generally speaking, the more attributes a person shares with individuals who have committed terrorist attacks or other offences or individuals who are considered to be likely to perform such acts in the future, the more likely that person becomes to be singled out by profiling measures. For example it is highly likely that as a result of profiling a young Muslim male travelling alone without checking in any luggage will be perceived as a risk to aviation security, whereas an elderly Christian woman will not be perceived as a risk. As a result, profiling measures like those in operation at airports in the United States of America have been heavily criticised: 'The behavior detection program is no longer a behavior-based program, but it is a racial profiling program.'[245]

Passenger profiling

Passenger groups relating to certain attributes	**Security practices and situations**	**Related freedoms**
Gender	*using past terrorist attacks as reference:* women will be less likely to be affected by passenger profiling, since past terrorist attacks were executed predominantly by males	presumption of innocence, privacy and data protection, equal treatment and non-discrimination; additional freedoms are affected by measures resulting from being singled out

[244] For more in-depth descriptions of profiling see D2.1 and D2.2 of the SIAM project.

[245] *Schmidt, M. S./Lichtblau, E.*, Racial Profiling Rife at Airport, U.S. Officers Say, The New York Times, 12.8.2012, New York, A1. Cf. *Schmidt, M. S.*, Report Says T.S.A. Screening Is Not Objective, 5.6.2013, New York, A17.

		by profiling
Age	*using past terrorist attacks as reference:* small children and the elderly are unlikely to be affected by passenger profiling; most terrorists have been relatively young (mostly between 18 and 35 years old) which means that profiling will target this age group	presumption of innocence, privacy and data protection, equal treatment and non-discrimination; additional freedoms are affected by measures resulting from being singled out by profiling
Purpose of travel	*using past terrorist attacks as reference:* business travellers are less likely to be affected than other travellers due to their overall appearance (e.g. wearing suits, expensive clothing and accessories) and the fact that they travel frequently without incident	presumption of innocence, privacy and data protection, equal treatment and non-discrimination; additional freedoms are affected by measures resulting from being singled out by profiling
Nationality	*using past terrorist attacks as reference:* nationality can greatly affect the impact of profiling; being a foreigner may be enough to raise suspicion; where in the past terrorists have come from certain countries, this may affect all passengers from such a country; *using behaviour as reference:* foreigners may exhibit innocuous behaviour that is misinterpreted as suspicious or dangerous by the system	presumption of innocence, privacy and data protection, equal treatment and non-discrimination; additional freedoms are affected by measures resulting from being singled out by profiling
Race	*using past terrorist attacks as reference:* passenger profiling is always in danger of becoming racial profiling, especially in a society where terrorists are mostly perceived as being members of a certain race	presumption of innocence, privacy and data protection, equal treatment and non-discrimination; additional freedoms are affected by measures resulting from being singled out by profiling

Religion	*using past terrorist attacks as reference:* clothing, accessories and skin colour may reveal a person's religion; any type of profiling that highlights members of certain religions or religious groups as security threats will have a profound impact on members of these groups; *using behaviour as reference:* members of certain religions may exhibit behaviour that is misinterpreted as suspicious or dangerous by the system	presumption of innocence, privacy and data protection, equal treatment and non-discrimination; additional freedoms are affected by measures resulting from being singled out by profiling
Disability	*using past terrorist attacks as reference:* persons with disabilities are less likely to be singled out as a result of profiling; this could change however, if a terrorist attack occurred where the attackers hide prohibited articles in artificial limbs, wheelchairs or the like; *using behaviour as reference:* see above under the heading 'Smart CCTV'	presumption of innocence, privacy and data protection, equal treatment and non-discrimination; additional freedoms are affected by measures resulting from being singled out by profiling
Other	*using other social characteristics as reference:* profiling may also be based on other attributes, the most prominent being the overall outward appearance of a person (e.g. type of clothing, personal hygiene), thus highlighting certain social groups; *using behaviour as reference:* persons who behave differently from the norm for certain reasons beyond those mentioned above (e.g. fear of flying, social anxiety) will be more affected than those who do not exhibit such deviations from the norm	presumption of innocence, privacy and data protection, equal treatment and non-discrimination; additional freedoms are affected by measures resulting from being singled out by profiling

Profiling illustrates that it is impossible to assess the intrusiveness of an abstract measure or category of SMTs since the concrete design of the SMT has to be known in order to make an assessment. Profiling for instance can come in many shapes and forms. It can range from police or security officers watching people for suspicious behaviour in a public space to the processing of large amounts of personal data.

Scope and intrusiveness can thus vary greatly depending on the concrete modus operandi of the SMT. Likewise, smart CCTV can include a number of features like tracking a person, behaviour analysis or plate number recognition, but it does not necessarily have to. Hence, it is also impossible to make a legitimate statement about the intrusiveness of an SMT in relation to certain groups of passengers. However, more general statements like the abovementioned can be made.

Ultimately, the level to which individual passenger groups are affected by SMTs depends on the level of protection that is granted by the respective legal system in combination with certain factors that are unique to a specific SMT.

Another important factor has to be kept in mind: The ability to exercise a right is highly dependent on a passenger's individual level of information. Different groups of passengers will have a different level of information. For instance, a frequent flyer may possess more information on aviation security than a person who only flies occasionally, because as a frequent flyer, he or she will have frequently been subjected to a vast variety of security measures. On the other hand, a frequent flyer who is enrolled in a trusted traveller programme may be less familiar than a person who is not enrolled in such a programme because as a result of being enrolled in such a programme certain SMTs may be omitted during a security check. Children will possess little to no information and have to rely on the level of information of their parents or legal guardians in order to exercise their rights. Foreigners may find it difficult to gain access to information that is only available in the language of the country they have travelled to, thus putting this particular group at a disadvantage in this regard.

4.1.3 Conclusion

It has to be kept in mind that prohibiting discrimination is not a sufficient measure in itself. Rather, it must be possible to effectively and efficiently punish transgressions. This reinforces passengers' trust in a security regime and individual CITs.

As shown, SMTs may have quite a different effect on passengers depending on certain attributes which certain groups of passengers may have in common. When implementing CITs, these differences in effect should be considered, and CITs should be adapted or introduced into the security regime accordingly.

4.2 Employees

Employees can generally be affected by SMTs in three ways:

1. Employees are subjected to a reliability screening (background check) either:
    a. as applicants who apply for a job pertinent to mass transportation security,
    b. during their time of employment, or
    c. both.

    To be able to perform such a background check, data has to be gathered and analysed, including very sensitive data like criminal records. An example for such a check has been presented in chapter 3.3 of this deliverable.
2. Employees have to undergo a security check:
    a. when entering their workplace,
    b. when leaving their workplace, or
    c. when entering or leaving specific areas of their workplace.
3. Employees are under constant or partial surveillance at their workplace. This can occur either:
    a. because a surveillance system is specifically designed for the surveillance of employees (e.g. to prevent theft by employees or to monitor employee performance), or
    b. because an employee works in an environment that is under surveillance for other reasons (e.g. to safeguard employees against acts of violence; employees work in areas that are under surveillance for security reasons, for instance at a security checkpoint).

As bullet 3 b. shows, surveillance security measures can have a double purpose: a surveillance camera aimed at a security checkpoint can help maintain security at the checkpoint, but it can also be used to monitor employees stationed at the checkpoint, e.g. to evaluate their work performance. This leads to severe infringements of employee rights which have to be duly justified, and have to be balanced against legitimate objectives like the need to maintain a level of security.

In summary, it can be said that employees who work in mass transportation systems may be as affected by SMTs as passengers, and considering extensive background checks and the fact that their exposure to SMTs may be significantly greater in quantity, they may even be more affected than passengers. However, whether or not employees are less affected, equally affected or more affected than passengers ultimately depends on the concrete design of the security regime.

5. Recommendations

This chapter aims at giving basic recommendations on how to configure security regimes in order to ensure the utmost protection of passenger rights in the context of maintaining security in mass transportation systems.

A methodology that enables decision makers to perform a legal analysis of individual security measures has been presented in D9.2 of the SIAM project. In this context, D9.2 has shown that legislation is in need of concretisation, and the deliverable has provided guidance on how to perform such a concretisation in order to boil down legislative text to its meaning for a specified situation.[246]

This chapter will thus focus on more general recommendations that concern the overall design of on-site security regimes. These recommendations have been derived from the entirety of the research conducted over the course of work package 9 and the SIAM project as a whole.

- Isolated CITs are not sufficient to maintain a high level of protection of passenger rights. Instead, a security regime as a whole has to be taken into consideration with interlinking CITs.

- A circumvention of regulation is facilitated by a lack of oversight. Thus, regular and unannounced checks should be conducted in order to ensure that mandated CITs are in fact implemented and complied with on-site.

- Employees concerned with security matters should receive regular training on how to treat passengers and on the purpose and operation of CITs in order to achieve and maintain a high level of compliance with codes of conduct and to ensure that all employees realise the importance of CITs, which rights passengers have and how they can help to uphold these rights.

- Alternative screening options for passenger and employee screening should be offered. An example will illustrate the importance of offering alternatives: One person may object to being screened by a body scanner because that person does not want the shape of his or her naked body to be registered. That person may thus want to opt for another screening method like a search by hand. On the other hand, a member of the Sikh religion may welcome the possibility to be screened by a body scanner because that way he does not have to discard his turban. Offering alternatives may help alleviate the burden of balancing security and personal freedom, since every passenger

[246] Cf. also chapter 2.3 of this deliverable.

can chose for him- or herself which screening option he or she will be subjected to.

- Operators of public mass transportation infrastructure should draw up individualised codes of conduct as guidelines for all employees concerned with the operation of SMTs. The benefit of creating such codes is twofold: On the one hand those people responsible for designing the security regime are forced to give thought to the concrete operation of every individual SMT and to put themselves in the shoes of both SMT operators and the passengers that come into contact with SMTs. On the other hand, this gives security employees and operators concrete guidance on how to behave both in day-to-day operation and in difficult situations.

- Security regimes should be designed in a way that prevents SMTs from being misused for purposes unrelated to security, like monitoring employee performance or voyeurism.

- In any security regime, certain areas should be exempt from the use of SMTs in order to create refuge areas where passengers are free from surveillance.

- CITs should be built into security technologies wherever possible. Operators of SMTs should not be able to circumvent these built-in CITs, e.g. by bypassing or deactivating them, or by tampering with the device. When choosing between different SMTs for implementation in the context of mass transportation, SMTs with built-in CITs should be favoured over SMTs without built-in CITs.

- Passengers should be informed about security procedures as well as the rights they enjoy, including access to an on-site ombudsman. This information should be provided in several languages or in the form of pictograms in order to ensure that foreigners are equally well informed as native speakers.

This shows that reflexivity is a key component of the realisation of a security regime that respects passenger rights.

Security planners must put themselves into the shoes of ordinary passengers (including fringe groups) in order to understand and be able to think over the impact of a certain measure, as well as the impact of a security regime as a whole.

6. Unidirectional data management procedures in surveillance systems

The following chapter discusses unidirectional data management procedures as a means to control personal data in surveillance systems.[247]

How does data transmission function?

Data transmission is defined as the transport of data from the location of their acquisition to the location where they are processed (point-to-point).[248] The transmission of data is thus the process of transmitting data purposefully between a person and a data terminal or between two data terminals, be it unilateral or bilateral.[249]

In the context of data transmission, analogue transmission has to be differentiated from digital transmission depending on the type of signal used. Analogue transmission is based on signals whose parameters form variable information of a physical unit (for instance electric currents, voltage, and length). The signal is not interrupted in its chronological sequence, meaning that it is continuous.

In this mode of transmission, the terminals communicating with each other are linked through a connection with a defined bandwidth and modulation.

Modern data transmission however uses digital signals. Digital transmission is based on two discrete and sequential conditions called bits, which are usually represented by two electrical voltage potentials. These potentials are assigned the logical values 0 and 1. A transmission is encoded in a sequence of zeroes and ones.

Certain value ranges of the signal parameters correspond to a single character or symbol. The individual characters are separated from each other by finite intervals and transmitted in predetermined formats, transmission speeds and transmission units.

Another criterion for data transmission is data structure, meaning the chronological sequence of data. Where all bits that represent a character are transmitted at once through sub-channels, this is called parallel data transmission. In case of serial data transmission, the individual bits a character is made of are transmitted over a single channel in sequential order.

Next to the criteria mentioned, the direction of data transmission, the data format which is of relevance to synchronise data terminal and transmission unit, the

247 This chapter was in parts contributed by Ref. jur. *Robert Weinhold*.
248 Cf. Gabler Wirtschaftslexikon 2010, under the heading 'Datenübertragung'.
249 This sub-chapter has been derived from ITWissen, under the heading 'Datenübertragung'.

transmission mode meaning data coding, and transmission speed play a pivotal role.[250]

Data transmission can be further differentiated between bidirectional and unidirectional data transmission. Bidirectional data transmission means that signals can flow in both directions. A participant can thus be both sender and receiver of transmissions.[251] In case of unidirectional data transmission, signals can only flow in one direction. A participant is thus limited to being a sender or a receiver, but not both. Typical unidirectional transmissions are broadcast transmissions like radio and television. [252]

How does CCTV function?

Before discussing the impact of using unidirectional data management in the context of surveillance systems, a short explanation of the term will be given, using German law as a reference.

a. What is surveillance?

According to the definition developed by *Dandeker*, in practice, surveillance consists of at least one of the following three elements: Collecting and storing information about persons and/or things, controlling the action of persons and/or machines and supervising their activities, and the affected persons following instructions given.[253]

b. What is video surveillance?

A universally accepted definition of the term 'video surveillance' does not exist. One possible definition is the one used in § 6b of the German Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG).[254]

Following § 6b(1) of the Federal Data Protection Act, video surveillance means monitoring an area using optic-electronic devices. The act allows for the surveillance of 'publicly accessible areas' using such devices 'as far as necessary for public bodies to perform their duties, to exercise the right to determine who shall be allowed or denied access, or to pursue legitimate interests for specifically defined purposes, and there are no indications of overriding legitimate interests' of the persons being put under surveillance.[255]

---

250 Cf. *Lipinski* 1996, 138.
251 Cf. *Lipinski* 1996, 72.
252 ITWissen, under the heading 'unidirektional'.
253 *Dandeker*, as quoted in *Glatzner* 2006, 6.
254 BGBl. 2003 I 66.
255 A list of other legal acts and principles that authorise the use of video surveillance can be found in *Scholz*, in: Simitis 2011, § 6b BDSG, para. 153 ff.

(a) Optic-electronic devices

The term 'optic-electronic devices' was purposefully chosen by lawmakers, in order to provide a neutral nomenclature which encompasses a wide range of devices.[256] Any device that can be used for the purpose of optical surveillance can be subsumed under it. It is thus irrelevant, how the device is designed and what features it possesses, for instance if there is a tilt and/or zoom functionality or if the device is stationary or mobile.[257] This also means that the term does not encompass dummies, i.e. objects that merely look like a surveillance camera without offering any actual functionality.[258] The main characteristic of an optical-electronic device is the conversion of light into electrical signals.[259]

(b) Monitoring

Monitoring is defined as the visualization of events and persons using adequate technical devices; monitoring is a form of surveillance.[260] Monitoring requires the registering of someone or something optically for a certain duration.[261] This means that it is not necessary that the device records anything, that the pictures created are analysed or that an analysis is even intended.[262] However, the term requires that personal data are collected.[263] § 3(1) of the German Data Protection Act defines personal data as follows: 'Personal data shall mean any information concerning the personal or material circumstances of an identified or identifiable natural person.' The question is whether data collected without any ancillary information contain such a personal reference. This is the case if a person's identity can be determined from such an image. A person's identity is not determinable where the risk of determination is so low that it becomes irrelevant.[264] This definition corresponds to Art. 2(a) of the European Data Protection Directive[265] which defines personal data as 'any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly'.

Thus, there is no video surveillance in terms of § 6b(1) of the Federal Data Protection Act, if no personal data is collected, which is the case with cameras that only produce images that do not allow for an identification of persons shown on these images, for instance overviews of a public area.

---

256 *Scholz*, in: Simitis 2011, § 6b BDSG, para. 36.
257 *Scholz*, in: Simitis 2011, § 6b BDSG, para. 36 f.
258 *Scholz*, in: Simitis 2011, § 6b BDSG, para. 41.
259 *Scholz*, in: Simitis 2011, § 6b BDSG, para. 38.
260 *Scholz*, in: Simitis 2011, § 6b BDSG, para. 63.
261 *Scholz*, in: Simitis 2011, § 6b BDSG, para. 64.
262 *Scholz*, in: Simitis 2011, § 6b BDSG, para. 65.
263 *Scholz*, in: Simitis 2011, § 6b BDSG, para. 66.
264 *Damann*, in: Simitis 2011, § 3 BDSG, para. 23.
265 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, L 281/31

What is unidirectional data transmission?

Unidirectional means 'in one direction'. In the context of data transmission, it means that a communication channel only allows for transmissions in one direction without a return channel.[266] Thus the recipient of a message is unable to confirm the receipt of the message. Since the recipient of a unidirectional transmission has no means of confirming that the transmission does not contain any errors, transmission mechanisms are more complex than is the case with bilateral transmission.[267]

How can unidirectional data management be used in the context of video surveillance?

The main characteristic of a video surveillance system as the 'technological equivalent of an on-site policeman'[268] is that images are captured by a video camera and then sent to a second location

- to store the images,[269]
- to be displayed to an operator,
- to be analysed by a specialised software,
- or any combination of the above.

To realize this main characteristic, unidirectional data transmission would be sufficient, since the only requirement to achieve this is that images can be sent from one location to another. Any data flow in the opposite direction is not primarily required. Since in a unidirectional system data may only flow from the camera to a second location but not vice versa, a person who gains access to the data connection cannot access any data stored at the second location, i.e. surveillance footage stored for whatever reason is secure from an attack from this side. However, a unidirectional network would still allow an intruder to intercept camera images.

A video surveillance system may also feature the following, optional characteristics. A video surveillance system may allow the operator to interfere with the camera by

- zooming,
- tilting the camera, and/or
- using a communication system in connection with the video surveillance system, e.g. by activating an intercom system or by pressing an alarm that will sound at the location of the camera to deter offenders.

A unidirectional system that eliminates all communication from the operator to the camera would eliminate these means to interfere with the camera, its environment

266 ITWissen, under the heading 'unidirektional'.
267 ITWissen, under the heading 'unidirektional'.
268 *Pieroth/Schlink/Kniesel* 2012, § 14, para. 92.
269 The storage unit may also be integrated into the camera.

and the persons whose images are being captured by the camera. Particularly the prevention of zooming and tilting the camera would greatly limit possibilities for an operator to misuse the camera in the context of voyeurism. However, it would also bar the operator from zooming in or tilting the camera in order to better identify a suspected criminal, to identify a presumably dangerous object, or to evaluate a situation better.

While the use of unidirectional data management would thus enhance data protection and privacy, eliminating possibilities to interact with the camera and the persons whose images are being captured by the camera may have a detrimental effect on security.

Thus, the main advantage of unidirectional data transmission compared to bidirectional transmission lies in the fact that due to an elimination of all means of an operator to affect the camera, certain privacy issues can be resolved. In the course of a proportionality test, this could benefit the chances of a surveillance measure to be deemed proportional.

In summary, the results of the use of unidirectional data management are the

- improvement of data security, the
- elimination of all possibilities of the operator to interact with the camera, and the
- elimination of all possibilities of the operator to interact with the persons whose images are captured by the camera.

Do legal specifications exist that regulate or demand the use of unidirectional data management in the context of video surveillance?

As was shown above, there are no legal requirements to use unidirectional data management in the context of video surveillance. The main reason for this is that lawmakers rarely dictate technological solutions, but rather use a technology neutral nomenclature that encompasses a wide array of technical devices. This ensures that laws do not have to be changed with every technological innovation.

7. Topics, aspects and Questions

As a result of these findings, we recommend that the following topics, aspects and questions should be implemented in the Assessment Support Tool produced in the SIAM project. The following list is not a complete enumeration of topics, aspects and questions relating to the basic rights and the protection of passenger rights since many have already been introduced into the Assessment Support Tool at an earlier stage of the SIAM project.

Topic	Aspect	Question
Passenger Rights	Information of Passengers	Are there signs that indicate that the SMT is in operation?
		Are there any obligations to inform passengers?
		Are passengers informed about the data protection standards in use?
		Are passengers familiar with a certain security technology? If a new technology is introduced, are passengers informed about the features of this technology?
		Have language barriers been taken into account?
		Are passengers made aware of their rights (e.g. redress, legal protection, legal actions)?
Passenger Rights	Complaints	Do passengers have the ability to file a complaint against the use of the SMT / their treatment?
		Is redress possible?
Transparency	Visibility	Is the structure of SMTs transparent?
		Can passengers comprehend which SMTs are used in which manner and context?
		Can the structure of SMTs be revealed to the public without sacrificing the integrity of the security concept as a whole?
		Is the purpose of the SMT clear to passengers?
Data Accountability	Oversight	Is there a data protection officer that helps to ensure compliance with data protection laws?
		Is the neutrality / independence of the data protection officer ensured?
Compliance	Voluntary	Are there any voluntary standards that give

	Standards	recommendations on how to use a certain SMT?
		Would it be beneficial to adhere to voluntary standards in order to increase passenger acceptance?
	Compulsory Standards	Are there any changes in the legal framework forthcoming that might affect the use of SMTs?
Discrimination	Equality	Are certain groups of people more likely to be affected by an SMT?
		Are measures in place that ensure that profiling is performed within the boundaries of the law? What are these measures?
	Religion	Does the SMT violate religious rules?
Compulsion	Refuge Areas	Are there areas that are of minimal relevance to security where people can be free from surveillance? Do unobserved areas remain?
		Can passengers distinguish between areas where SMTs are in operation and areas that are free from SMTs?
Scope of SMT	Location	Which degree of surveillance is necessary for which area?
	Manpower Requirements	How many persons are involved in the operation of the SMT?
Intrusiveness	Alternatives	Is a less intrusive SMT available that can perform the desired task at a comparable level?
Data Collection	Data Avoidance	Can the purpose of the SMT be fulfilled without gathering personal data?
	Type of Data	Does the SMT gather personal data that is not relevant to fulfilling its primary function?
		Does the data being collected by the SMT have to be personal data? Is it possible to omit references to a person?
		Does the SMT gather data that can be used for profiling / to create movement profiles?
		Is information about a passenger's health collected?
Data Storage	Data Reference	Is personal data anonymized or pseudonymized?
Data Processing	Data Analysis	Is it possible to process personal data through automatized processes, i.e. without involving human operators?
Scope of SMT	Location	Do bystanders have the ability to watch the

		SMT being used / a person being subjected to the SMT?
	Privacy	Are intimate details / secrets /disabilities revealed by the SMT?
		Does the SMT require passengers to (partially) undress?
	Function Creep	Can the SMT be used for purposes other than maintaining security?
Protection of Employees	Dual Function of SMT	Can an SMT that is used for passenger checking be used in a way to monitor employees?
Usability	Accessibility	Does the use of the SMT cause specific problems when dealing with children, disabled persons, the elderly or pregnant women?

References

Department for Transport, Airport Security: Report by Rt Hon Sir John Wheeler JP DL, London, 2002 (nicht veröffentlicht); cited: Department for Transport 2002.

Department for Transport, Access to Air Travel for Disabled Persons and Persons with Reduced Mobility – Code of Practice, London, 2008; cited: Department for Transport 2008.

Department for Transport, Airport Security Planning Quick Guide, London, 2010; cited: Department for Transport 2010.

Department for Transport, Better regulation for aviation security consultation document, London, 2011; cited: Department for Transport 2011.

Department for Transport, Code of Practice for the Acceptable Use of Security Scanners in an Aviation Security Environment, London, 2011; cited: Department for Transport 2011a.

Department for Transport, Accessible Train Station Design for Disabled People: A Code of Practice, 3. Aufl., London, 2011; citede: Department for Transport 2011b.

Department for Transport, Security in Design of Stations Guide, London, 2012; cited: Department for Transport 2012.

Dreier, H., Grundgesetz, Commentary, Vol. I (Art. 1-19), 3rd Edition, Tübingen, 2013; Vol. II (Art. 20-82), 2nd Edition, Tübingen, 2006; cited: *Author*, in: Dreier.

Drewes, M./Malmberg, K. M./Walter, B., Bundespolizeigesetz, 4th Edition, Stuttgart, 2010.

Freitas, P. J., Passenger aviation security, risk management, and simple physics, Journal of Transportation Security 2/2012, 107-122.

Gabler Wirtschaftslexikon, 17th Edition, Wiesbaden, 2010.

Gerrard, G./Thompson, R., How many cameras are there in the UK?, An exclusive report by the ACPO lead on CCTV, CCTVImage 42/2011, 10-12.

Giemulla, E. M., Das Luftsicherheitsgesetz, in: Möllers, M. H. W./van Ooyen, R. C. (Ed.), Europäisierung und Internationalisierung der Polizei, Vol. 3, Deutsche Positionen, Yearbook Öffentliche Sicherheit, 3rd Edition, Frankfurt am Main, 2011, 95-128.

Giemulla, E. M./Rothe, B. R., Recht der Luftsicherheit, Berlin/Heidelberg, 2008; cited: *Author*, in: Giemulla/Rothe 2008.

Giemulla, E. M./van Schyndel, H., Luftsicherheitsgesetz, Commentary, 1st Edition, Neuwied, 2006; cited: *Author*, in: Giemulla/van Schyndel 2006.

Glatzner, F., Die staatliche Videoüberwachung des öffentlichen Raumes als Instrument der Kriminalitätbekämpfung, Spielräume und Grenzen, Münster, 2006.

Grießler, E./Hauskeller, C./Lehner, D./Metzler, I./Pichelstorfer, A./Szyma, A., Stammzellen und Embryonenschutz – Status quo, Rechtsvergleich und öffentliche Debatte am Beispiel ausgewählter europäischer Staaten, Endbericht, Studie im Auftrag des österreichischen Bundeskanzleramts, September 2008, Institut für höhere Studien (IHS), Wien, 2008, http://www.bka.gv.at/DocView.axd?CobId= 32188; cited: *Grießler et al.* 2008.

Hobe, S./v. Ruckteschell, N., Kölner Kompendium des Luftrechts, Vol. 2 – Luftverkehr, Köln, 2009; cited: *Author*, in: Hobe/v. Ruckteschell 2009.

House of Commons, Home Affairs Committee, Counter-Terrorism Measures in British Airports, Ninth Report of Session 2009-10, 24.3.2010, HC 311, London, 2010; cited: House of Commons 2010, HC 311.

House of Commons, Transport Committee, Land transport security – scope for further EU involvement?, Eleventh Report of Session 2012-13, Vol. 1, 11.3.2013, HC 875, London, 2013; cited: House of Commons 2013, HC 875.

House of Commons, Transport Committee, Aviation strategy, First Report of Session 2013-14, Vol. 2, 10.5.2013, HC 78-II, London, 2013; cited: House of Commons 2013, HC 78-II.

ITWissen, Online-Lexikon für Informationstechnologie, www.itwissen.info.

Jarass, H. D./Pieroth, B., Grundgesetz für die Bundesrepublik Deutschland, Commentary, 12th Edition, Münster, 2012.

Leininger, C., Das neue Luftsicherheitsrecht der Europäischen Union, Entwicklungen und Änderungen durch Inkrafttreten der Verordnung (EU) Nr. 185/2010, Part I, ZLW 3/2010, 335-361.

Leininger, C., Das neue Luftsicherheitsrecht der Europäischen Union, Entwicklungen und Änderungen durch Inkrafttreten der Verordnung (EU) Nr. 185/2010, Part II, ZLW 4/2010, 485-512.

Lienhart, I., Luftsicherheit im europäischen Kontext: Die Revision der Verordnung (EG) Nr. 2320/2002, ZLW 1/2009, 1-15.

Lipinski, K., Lexikon der Datenkommunikation, 4th Edition, Bonn, 1996.

v. Mangoldt, H./Klein, F./Starck, C., Kommentar zum Grundgesetz, Commentary, Vol. 1, Präambel – Art. 1-19, Vol. 2, Art. 20-82, 6th Edition, München, 2010; cited: *Author*, in: v. Mangoldt/Klein/Starck.

Maunz, T./Dürig, G., Grundgesetz, Commentary, established by Theodor Maunz and Günter Dürig, published by Roman Herzog, Rupert Scholz, Matthias Herdegen and Hans Klein, 67th Edition, München, 2012; cited: *Author,* in: Maunz/Dürig 2012.

National Policing Improvement Agency, Reference Handbook, Guidance on Policing at Airports, London, 2011; cited: National Policing Improvement Agency 2011.

Pieroth, B./Schlink, B./Kniesel, M., Polizei- und Ordnungsrecht mit Versammlungsrecht, 7th Edition, München, 2012.

Richter, S., Luftsicherheit, Einführung in die Aufgaben und Maßnahmen zum Schutz vor Angriffen auf die Sicherheit des zivilen Luftverkehrs, 3rd Edition, Stuttgart, 2013.

Roggan, F./Kutscha, M., Handbuch zum Recht der Inneren Sicherheit, 2nd Edition, Berlin, 2006; cited: *Author*, in: Roggan/Kutscha 2006.

Ronellenfitsch, M., Terrorismusbekämpfung und Datenschutz, JurPC Web-Doc. 115/2007, para. 1-113, http://www.jurpc.de/jurpc/show?id=20070115.

Sachs, M., Grundgesetz, Commentary, 6th Edition, München, 2011; cited: *Author*, in: Sachs 2011.

Simitis, S. (Ed.), Bundesdatenschutzgesetz, Commentary, 7th Edition, Baden-Baden, 2011; cited: *Author*, in: Simitis 2011.

Walker, C., Terrorism and the Law, Oxford, 2011.