Chapter 5
Legal Principles of Privacy and Data Protection

5.1 Introduction

As discussed in Chap. 4, the states are obliged to ensure the security of civil aviation and have the right to establish security procedures that they believe are necessary. However, this does not mean that security agencies are free to do anything. In addition to the aviation security considerations discussed in Chap. 4, such as threats and risks, costs and benefits, etc., there are other mechanisms to review the operations of aviation security agencies, for the purposes of this research – in the terms of privacy and data protection. The principles of privacy and data protection can serve as such mechanisms.

Since technological development is rapid, and legislation is not, and since there is a lack of laws on every specific aviation security technology, it may be more fruitful, instead of analysing existing regulations with reference to every aviation security measure, to apply privacy and data protection principles on a case-to-case basis. The point is that principles provide a normative rationale for judging the acceptability of surveillance, on the basis of which opposition or adaptation may take place.[1] They express the essence of privacy/data protection values and constitute the basis of the applicable regulation, allowing identification of exact privacy/data protection concerns that arise as a result of concrete aviation security measures and how these can be dealt with.

Legal principles are important in other dimensions too. As some researchers suggest, in the world of the increasingly global and interactive market, increasing connectivity among jurisdictions, legal professions and doctrinal disciplines, there should be more emphasis placed on legal principles as a tool in modern legal training.[2] When assessing aviation security measures as a complex and global network,

[1] Wright et al. (2015) p. 288.

[2] Cankorel. *Cognitive Classification of Legal Principles: A New Approach to International Legal Training*. In: Ankara Law Review. Vol. 5 (2008) p. 154.

O.M. Enerstvedt, *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles*, Law, Governance and Technology Series 37, DOI 10.1007/978-3-319-58139-2_5

with illustrations from a number of selected states, it would be too complicated and insufficient to take into account national privacy/data protection law separately for each measure.

Thus, for research such as the present study, which entails various disciplines, jurisdictions and languages, the analysis of applicable legal principles has a pragmatic goal: it is intended to suggest an effective universal (common, general) model for approaches to the aviation security-versus-privacy dilemma, for any jurisdiction and any legal regime.

Accordingly, this chapter is dedicated to the core legal principles of privacy and data protection which are the key elements for this research, since they will constitute a practical tool for evaluation of concrete aviation security measures in the Special Part.

As I mentioned in Chap. 1, in the search of concrete principles and determination of what the legal principles are, I was faced with a number of methodological difficulties and endeavoured to formulate my own approach to principles. The main condition is that principles for this research are *legal* principles. In contrast to *political* principles, these legal principles must be contained in the law. In addition, they can be formulated and applied by courts.

5.2 What Are Principles in This Research?

In general, legal principles constitute the original, defining ideas, positions, attitudes that make up the moral and organizational basis for the appearance, development and operation of the law; they express the essence of law: what the law consists of, what it should be focused on and concentrated in its development.[3] It is common to make a distinction between legal rules and legal principles; however, there are many approaches to formulating what the principles are.

Some philosophers, in particular Dworkin, believe that the principles play a crucial role in the law.[4] Others "attack" principles, for instance by treating them as binding upon judges or as summaries of judges when the latter are forced to go beyond binding standards.[5] They claim that via Dworkin's interpretation, rules in effect are dropped "out of the picture, leaving the field to principles".[6]

Nevertheless, as Alexy notes, two main positions can be differed: (1) principles express the idea of optimization; they are optimization commands, and it is this feature that differs them from the rules, (2) the optimization thesis is wrong.[7] But after exploring different views, Alexy concludes that no explanation of what

[3] Matuzov. *The theory of state and law: lectures.* (2001) pp. 83–86.

[4] Raz. *Legal principles and the limits of law*. In: Yale Law Journal (1972) p. 824 referring to Dworkin. *The model of rules*. In: The University of Chicago Law Review (1967).

[5] Dworkin (1967) p. 31.

[6] Alexander and Kress. *Against legal principles*. In: Iowa L. Rev. Vol. 82 (1996) p. 739.

[7] Alexy. *On the structure of legal principles*. In: Ratio Juris. Vol. 13 (2000) p. 294.

principles are "is more promising than a construction of them as obligations to be optimized, where this corresponds to obligations to optimize. This construction seems to be the best expression of the idea of an ideal "ought" "and of ideal validity".[8]

I have stated repeatedly that principles are essential for this work. I will focus on explaining the essence and role of principles rather than debating whether principles as such are important or not.

There are a number of differences between rules and principles. First of all, the traditional approach indicates first of all the formal binding effect (legal rules have them, but not the principles). However, today, the principles also may be expressed in written norms[9] and have binding effect, thus, legal principles are sources of law. Like other laws, they can be enacted or repealed by legislatures and administrative authorities and can become legally binding via establishment by the courts.[10]

For instance, with reference to data protection principles, although they are primarily abstractions, they simultaneously "have a normative force of their own".[11] This force is achieved in three ways: (i) they are expressly incorporated in data protection laws as rules[12] automatically giving them legal force, (ii) they are guiding standards in interest-balancing processes, and (iii) they shape drafting of new data protection legislation.[13]

Accordingly, due to their connection to overriding values and aims, legal principles may have very practical force, including normative force: they may serve as sources for emerging legal norms; they may contribute to organize and coordinate arguments around a legal question[14] as well as serve as guiding standards in interest-balancing processes (in our case, security versus privacy).

The second difference relates to the logical character and content. Principles are abstractions and imply more general, fundamental norms of a legal order (norms of general application that do not take into account specific legal facts[15]), while legal rules imply concrete provisions.[16] Accordingly, if the facts of a case are such that the conditions of application of a valid legal rule have been met, then the rule must be applied; if they have not been met, then the rule cannot contribute to the case.[17] In

[8] *Ibid.* p. 304.

[9] Black. *Regulatory conversations*. In: Journal of Law and Society. Vol. 29 (2002) p. 172.

[10] Raz (1972) p. 848.

[11] Bygrave (2014) p. 145.

[12] See DPD Articles 6, 7, 10–12, 16–17, 22–23; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) Paragraph 14; the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981).

[13] Bygrave (2014) p. 145.

[14] Malt. *Sameirettslige Prinsipper* In: Selskap, kontrakt, konkurs og rettskilder (2010) p. 183.

[15] Muñiz. *Legal Principles and Legal Theory*. In: Ratio Juris. Vol. 10 (1997).

[16] Petersen. *Customary Law without Custom-Rules, Principles, and the Role of State Practice in International Norm Creation*. In: Am. U. Int'l L. Rev. Vol. 23 (2007). p. 287.

[17] Perry. *Two models of legal principles*. In: Iowa L. Rev. Vol. 82 (1996) p. 788.

contrast to that, while principles can be unable to solve a concrete case, they may assist in practical reasoning, about what ought to be done.[18]

As for the content, principles are often indistinguishable from various values, interests, rights, policies and goals (i.e. have value-oriented content), while rules mainly specify concrete actions for particular circumstances (action-oriented).[19]

This nature of principles presents both advantages and disadvantages. The abstract nature of principles facilitates legal analysis: an expert in these abstractions analyses legal problems more efficiently than a novice who takes concrete and inefficient steps.[20] This is another advantage of using principles as the basis of evaluation in this research.

However, the principles are formulated broadly and not specifically, thus, their legal effect may be uncertain. For proper application in practice, in order to be applied to specific cases with correct results, principles often require further interpretations and clarifications, and the approaches of different states and actors here may differ greatly.

Another result of the principles' general nature is that in the case of a conflict between principles and rules, the latter will often prevail as a more specific norm.[21] An exception is the proportionality principle, which will often defeat a rule. Nevertheless, the most important consequence for the terms of this research is that on the one hand, it is always possible to make exceptions and deviate from principles by a concrete legal rule. For instance, the principles can be restricted due to the aviation security needs. With regard to data protection, there are proposals to overcome this nature and adopt legislation to clarify the application of some key principles and include data protection principles in one comprehensive legal framework.[22] These initiatives may be helpful in the sense that they could solve some uncertainties and unclear issues, but they are not yet realized.

On the other hand, "principles can justify rules, but not vice versa".[23] If concrete legal norms contain exceptions and restrictions to privacy and data protection due to aviation security needs, in this situation, the principles are aimed to ensure that the restrictions are as limited as possible. Thus, principles in this case can be used to find a balance between security and privacy.[24]

Thirdly, principles are less prone to remain unchanged for a long time, because they are formulated in a general way, and because principles are starting points which presuppose the possibility of exceptions. In contrast to that, legal rules

---

[18] *Ibid.* p. 787.

[19] *Ibid.* p. 788.

[20] Cankorel (2008) p. 156.

[21] Alexy and Rivers. *A theory of constitutional rights* (2010) pp. 83–84.

[22] Article 29 Data Protection Working Party and the Working Party on Police and Justice. *The Future of Privacy. Joint contribution of the Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* (2009) p. 6.

[23] Perry (1996) p. 788.

[24] Aquilina (2010) p. 140.

usually correspond to a certain historical period. For instance, the data protection principles are likely to remain in the future revisions of the data protection laws. Despite the challenges provoked by new technologies and globalization, it is argued that the main principles of data protection are still valid.[25] At the same time, a negative consequence of this nature is that data protection principles do not fully address the surveillance issues, in particular those connected with new technologies and information systems.[26] As mentioned in Chap. 2, there are currently endeavours to modernize existing data protection law, and this concerns principles too. The aim is to keep the core essence of the principles, but update them according to new realities. Thus when discussing concrete data protection principles, I will take into account both existing rules and proposed.

Fourthly, many of the legal principles are transferrable in the sense that they transcend jurisdictional, professional and doctrinal boundaries.[27] This is particularly important for this work, which deals with numerous jurisdictions, levels and spheres (privacy and security) and at the same time needs to find proper connections between them. In this sense, common principles may help to unite all these pieces.

Finally, due to the connection with overriding values and aims, and because they are prone to internal organization within their abstract system, legal principles are teachable,[28] and application of principles provides room for dynamic and adaptive law.

All the above-mentioned features of legal principles determine the roles of principles of privacy/data protection and the tasks they fulfil. First, the principles of privacy/data protection unite legal rules, which may have different legal status and may be provided by various institutions, in a single legal system. They will allow determining "axioms" of privacy and data protection, in particular, common privacy and data protection standards and requirements for various aviation security techniques which can be applied universally.

Secondly, when new issues require legal regulation, the principles provide a good starting point. On the one hand, they can assist in developing regulation, or at least best practices and guidelines for the use of aviation security technologies, to provide information to regulators about how rights to privacy and data protection can be ensured. It is of course preferable that legal regulation – based on principles – should appear before any new aviation security procedure or amendment to existing procedure takes place. Accordingly, along with other considerations such as the aviation security measure's costs and benefits (see Chap. 4), effects on other human rights (Chap. 3), the principles of privacy/data protection should be taken into account before the measure is implemented. On the other hand, principles can

[25] Article 29 Data Protection Working Party and the Working Party on Police and Justice (2009) p. 6.

[26] Raab. *Surveillance: Extending the limits of privacy impact assessment* In: Privacy impact assessment (2012b) p. 379.

[27] Cankorel (2008) p. 154.

[28] *Ibid.* p. 156.

assist to evaluate if the existing legal regulation is adequate and sufficient, e.g. are all principles taken into account?

As discussed, in reality, the law usually goes behind the technology. Of course, as mentioned above, privacy/data protection principles may also face difficulties when addressing new technologies, but their advantage is that they can be applied in a broader, a more flexible way, taking into account the essence, the nature of the values they imply. As the result, in the situation of lack of regulation or non-regulation, principles can be applied to existing aviation security measures directly. Moreover, in the situation of lack of regulation or non-regulation, they may contribute to mechanisms of self-regulation, i.e. serve as guidelines for manufacturers, integrators, distributors, security experts, operators of aviation security technologies and other relevant actors.

Thirdly, principles may help in assessing the actions of these different stakeholders, especially those who are usually not subject to specific legal regulation such as data protection rules: security providers, security experts and so on.

Fourthly, principles may help educate the public about how privacy challenges associated with the use of these technologies are being addressed.

What is especially important for this research is that principles may help in evaluating a concrete aviation security measure at any stage of its development and lifetime. Hence, a practical task of the principles in this research is to serve as tests of particular security measures in the Special Part: taking into account technical characteristics and operation of the measure, they allow determining which concrete privacy/data protection concerns arise in the course of these concrete measures and, taking into account other factors such as effectiveness and other human rights concerns, evaluate whether the concerns are justified or not. Ultimately, therefore, principles can be used to evaluate whether aviation security regimes are lawful, necessary and proportionate. Accordingly, the principles will be a necessary tool for this research.

With reference to a number of issues, the use of the principles approach is already accepted formally. For instance, with regard to passenger data transfer from the EU, data protection principles are the key to determining whether the country requesting data can be considered as providing an adequate level of data protection. Sufficient compliance with data protection principles and procedural/enforcement requirements constitutes a minimum requirement for protection to be considered adequate.[29]

The main groups of principles discussed in this research are:

1. General principles
2. Principles of aviation security discussed in Chap. 4
3. Privacy principles
4. Data protection principles

[29] See Article 29 Data Protection Working Party. *Working Document. Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (1998).

Obviously, as will be discussed below, there exist overlays between all of these categories and there are also overlays between different principles within one group. Some of the selected data protection principles can hardly be considered as individual and/or wholly independent and separate from other principles. These overlays, as well as close relations between principles, indicate that the principles are interdependent, indivisible and interrelated in varying degrees.

It should be noted that concrete privacy principles in this chapter will be considered within either general or data protection principles. The point is, as discussed in Chap. 2, that the EU case law has formulated approaches on criteria of ECHR Art.8(2) (in accordance with the law, necessity, etc.). All these elements fall within or have close connection with either general or data protection principles.

Thus, below, two groups of principles will be discussed in more detail: general and data protection principles, with indication of possible connections and relations between each other. The lists of the discussed principles are not deemed to be exhaustive and present selected items, which, in my opinion, are critical for the security versus privacy dilemma.

5.3 General Principles

The first group comprises international general principles that are "a manifestation of international law".[30] International law here is understood as general or common international law, which is customary law valid for all states belonging to the international community.[31] Accordingly, these principles can also be defined as "generally recognized norms of international law of the most common character".[32] These principles are mandatory and contain obligations *erga omnes*, i.e., obligations of each and every member of the international community. They are stipulated in international legal instruments in different contexts, often repeated by national laws.

For instance, international general principles include such principles as *pacta sunt servanda*, the principle of state sovereignty, equality of states, legality, proportionality, etc. They are universal and valid in any sphere, from application to any human right to the basics of international air law: these principles will apply no matter where the aircraft is flying. These principles are applied by courts when determining the lawfulness of legislative and administrative measures of the states.

In this research, three of international general principles play important role for the aviation security versus privacy dilemma: legality, proportionality, equality and non-discrimination. While the latter was discussed in Chap. 3 together with the right to equality and non-discrimination, legality and proportionality will be analysed in more detail in this section.

---

[30] Voigt. *The Role of General Principles in International Law and their Relationship to Treaty Law*. In: Retfærd. Vol. 31 (2008). p. 5.

[31] Kelsen. *Principles of international law* (1952) p. 19.

[32] Bordunov (2007) p. 39.

5.3.1 Legality

5.3.1.1 Introduction

In general, aviation security measures may fit into a democratic, rule-of-law society if such systems comply with the fundamental legal requirements of such societies.[33] As mentioned above, the principle of legality is paramount in democratic society and it is a basis of any other principles. It is enshrined in the majority of international conventions and treaties as well as national laws.

The legality principle is closely related to the concepts of legal formalism and the rule of law. It implies that states should be governed by law. For instance, law enforcement agencies must observe the rule of law, whereby all acts of law enforcement agencies have to comply with the law and such acts cannot be carried out outside the limits and boundaries delineated by the law.[34] Accordingly, the law must be clear, ascertainable and no law must be given retroactive effect.[35] Hence, decision-makers must apply legal rules that have been declared beforehand, and not alter the legal situation retrospectively by discretionary departures from established law.[36]

In Norwegian law, for instance, the principle of legality ("legalitetsprinsippet") enjoys constitutional status; it is an unwritten norm requiring that actions by public authorities that infringe significantly on the rights and freedoms of private citizens (e.g. police surveillance), be authorised by statute.[37] Moreover, "no one may be sentenced except according to law, or be punished except after a court judgment. Everyone has the right to be presumed innocent until proved guilty according to law".[38]

With reference to the aviation security, the principle of legality applies directly. For instance, Russian laws stipulate that legality is a principle of transport security,[39] general security,[40] as well as a principle of anti-terrorism activities.[41] Clearly, aviation security decision-makers must apply legal rules that have been declared beforehand; all acts of security agencies must comply with the law, and the decisions establishing security measures or techniques as well as their practical implementation should have basis in law. However, as mentioned in Chaps. 1 and 4, aviation security is characterized by a high amount of restricted information. This has direct effect on openness and transparency regarding legal information about aviation security.

---

[33] Wright et al. (2015) p. 290.

[34] Aquilina (2010) p. 141.

[35] Norwegian Constitution § 97.

[36] Wikipedia. Principle of legality. http://en.wikipedia.org/wiki/Principle_of_legality

[37] Bygrave (2001) p. 333.

[38] Norwegian Constitution § 96.

[39] RF Federal law of 9 February 2007 N 16-FZ On transport security, Art. 3(1).

[40] RF Federal law of 28 December 2010 N 390-FZ On security, Art. 2(2).

[41] RF Federal law of 6 March 2006 N 35-FZ On counteraction against terrorism, Art. 2.

In the privacy context, the term "in accordance with the law" (lawfulness) and "legitimate aim" are used as the conditions for limitation of the privacy right (Article 8(2) ECHR).[42] In data protection field, it is common to indicate the principle of lawful processing.

Below, important issues for this research will be analysed in more detail: (1) information openness and transparency (overlapping with the requirements of accessibility, foreseeability and specific, precise and clearly defined law within "in accordance with the law" and also with data protection transparency principle), (2) in accordance with the law, (3) legitimate aim, and (4) lawful processing.

5.3.1.2 Information Openness and Transparency

In general, *publicatio legis* principle implies that ideally, laws and other legal sources should be communicated to the citizens and/or published so that citizens can familiarize themselves with the laws and rules relating to them.

A closely related term is the transparency principle. As mentioned in Chap. 3, it requires that information provided to the public should be easily accessible and easy to understand; in other words, the information must have two attributes: clarity and accessibility. The states should be transparent about their actions, in particular, about the use and scope of surveillance techniques and powers.[43]

In general, transparency principle includes (i) transparency of legal rules on aviation security practices, and (ii) transparency of the security practices. The latter is mandated to various degrees by legal rules, but it is distinct from the former type of transparency. In this section, the first type of transparency will be addressed. The second type will be mentioned in Sect. 7.2.2 where applicable in connection with legal transparency, since it is important for understanding the context and a broader picture. It will then be addressed in Sect. 8.2.4.3 in association with the notion of transparency in general – an important emerging legal principle.

The absence of legal information makes it impossible to fully realize individual rights, and it is the duty of the state to ensure its availability. One of the most important factors of availability of legal information is its quality: information should be scientific, objective, reliable, specific, complete, adequate, relevant, timeliness, optimal, accurate, and concise.[44]

Thus, in addition to a "negative" meaning of the legality principle – that the state powers must have a legal basis (see below), the legality principle also implies some "positive" obligations of the state – to ensure the availability of legal information. The importance of the latter cannot be underestimated since it may serve as a

[42] See Chap. 2.

[43] International Principles on the Application of Human Rights to Communications Surveillance, signed by 258 non-governmental organizations. Final version 10 July 2013. https://en.necessary-andproportionate.org/text

[44] Kovaleva (2007) p. 7.

safeguard for the rule of law, contributing to predictability, awareness, open political debate, etc.

Making legal information publicly available allows persons to become aware of the impact on their privacy and data protection rights as well as other human rights and gives them instructions concerning where to lodge a complaint in the event they believe their rights are violated, and provides them with the opportunity to redress. Moreover, transparency plays a positive role in public acceptance of aviation security technology: for instance, pursuant to a study from the UK, presenting passengers with information on body scanners results in positive increases in their acceptance of this technology.[45] The importance of this principle can be compared with the importance of the proportionality principle: "If we can only remember two concepts as regards the legislation on privacy, it needs to be these two [proportionality and transparency]".[46]

The researchers also use the terms (i) deliberation and (ii) awareness and communication. The former means that when new measures are being considered, or when existing schemes are being expanded, the deliberative and democratic process should be as open, consultative and fair as possible, while awareness and communication provide a platform for debate and change. They are already practiced by for instance DPAs.[47]

At the same time, according to categories of access, information can be divided into open (public) and restricted. Normally, the states issue Freedom of Information Acts (FOIA) entailing responsibility on the part of the state to provide public access to information held by public authorities.[48] In general, the intent of FOIA is to avoid unnecessary secrecy.[49] The core idea is that legal information, if not already available in open sources such as Internet, can be obtained by citizens via FOIA request.

FOIA provide exemptions which authorize government agencies to withhold information deemed to be restricted. In the USA, this pertains to information relating to national defence or foreign policy, information that is exempt under other laws, trade secrets and confidential business information, law enforcement records or information, etc.[50] Russian law provides a broad formulation, "restricted information".[51] Analysis of other laws allows us to infer that this includes state secrets[52] and confidential information such as personal data, information about

[45] Mitchener-Nissen [et al.] *Public attitudes to airport security: The case of whole body scanners.* In: Security Journal (2011).

[46] Poullet (2009) p. 224.

[47] Wright et al. (2015) p. 288.

[48] In the selected states, FOIA were enacted in the USA in 1966, in UK in 2000, in Norway in 2006, in Russia in 2009.

[49] UK ICO. What is FOIA? https://ico.org.uk/for-organisations/guide-to-freedom-of-information/what-is-the-foi-act/

[50] Title 5 of the US Code, section 552.

[51] Art.20(4) of Russian Federal law of 9 February 2009 N 8-FZ On providing access to information about the activities of government bodies and local authorities.

[52] See e.g. Russian Federal law of 21 July 1993 N 5485–1 On state secrets.

investigations and legal proceedings, service secrets, professional secrets, trade secrets, details of the invention.[53] Information about "the special means, techniques and tactics of the measures to combat terrorism as well as the composition of their participants"[54] is also confidential.

Thus, not all so-called public information can be made publicly available. As mentioned in Chap. 4, aviation security decision-making is not a democratic process, and as Chap. 6 will discuss, the details on the specific technologies and their *modus operandi* cannot be fully debated in a public forum.

In the case law in the area of combating terrorism, the ECtHR admitted that "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction".[55] The Court thus recognizes that intelligence – secret services – may legitimately exist.

The problem is that when invoking "security needs", security organs may apply broader restrictions than necessary, creating unnecessary secrecy. Thus, certain limits apply. In particular, pursuant to case law, secret surveillance is justified only in so far as it is strictly necessary for safeguarding the democratic institution: the Court, being aware of the danger inherent in secret surveillance measures "of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate".[56]

For instance, with regard to secret surveillance databases, in *Shimovolos v. Russia*,[57] the case concerned the registration of a human rights activist in a secret surveillance security database and the tracking of his movement as well as related arrest. The database in which his name had been registered had been created on the basis of a ministerial order which had not been published and was not accessible to the public. Therefore, people could not know why individuals were registered in it, what type of information was included and for how long, how it was stored and used or who had control over it.[58] Violation of Article 8 thus took place.[59] This means that despite security needs, some transparency still requires.

In *Khan v. the United Kingdom*, the Court found that it was not in accordance with law that the law did not exist and the rules were not directly publicly accessible[60] – i.e. it was presumed the rules could be open to the public.

---

[53] Presidential decree of 6 March 1997 N 188 On approval of the List of confidential information (Russia).

[54] Federal law of 6 March 2006 N 35-FZ On counteraction against terrorism, Article 2 (10).

[55] *Klass and others v. Germany*, No. 5029/71, 6 Sept 1978, §42.

[56] *Ibid.* §49.

[57] *Shimovolos v. Russia*, No. 30194/09, 21 June 2011.

[58] *Ibid.* §69.

[59] *Ibid.* §71.

[60] *Khan v. the United Kingdom,* No. 35394/97, 12 May 2000, §27.

Thus, air passengers should have information about the aviation security technologies/methods used as well as their consequences. Of course, it would be impossible to provide all the details of the technology capabilities, but general information to the extent that it does not jeopardize the security should be provided. This idea is stipulated in the Norwegian Personal Data Act 2000, for instance: the controller must inform a person of "the security measures implemented in connection with the processing insofar as such access does not prejudice security".[61] But, a problem emerges in determining what information jeopardizes security and what does not. Similar to any security decisions, it is not a democratic process, and it is the security organ who decides. Thus, there may always be a tendency to keep secret as much information as possible under the pretext of ensuring the safeguarding of security.

Accordingly, in practice, secrecy, either necessary or unnecessary, creates a problem for realization of the principle of transparency. Additionally, there may appear problems with such requirements of "in accordance with the law" criteria as accessibility of law, foreseeability of interference; precise, specific and clearly defined law (see below).

5.3.1.3 In Accordance with the Law

The criteria "in accordance with law" implies, first, that any limitation, any interference must have a legal basis ("some basis in domestic law").[62] No security measure that interferes with human rights can be adopted in the absence of an existing publicly available legislative act. For instance, the ECtHR held that the use of a covert listening device by the UK authorities was not in accordance with law because there was no statutory system to regulate the use of such devices. The latter was governed by Home Office Guidelines which were neither legally binding nor directly publicly accessible.[63] Two aspects can be seen here: first, it is not enough to follow a voluntary code of practice, internal guidelines, etc., and any security measure should be subject to legal regulations. Secondly, the formulation "directly publicly accessible" implies that the Court considered that the respective rules could refer to open rather than restricted information.

One of the main problems in aviation security is that changes in technology occur much faster than regulators can address those changes. Thus, as discussed in Chap. 4, it is quite common that a measure is established by a decision of executive body in the form of order, guidelines, etc. Of course, the latter may present some advantages such as more timely reaction to technological changes. Nevertheless, if an aviation security measure is not specifically authorized by law and is regulated only by administrative practice, it can hardly be legitimate.

---

[61] Section 18 (b).

[62] *Kruslin* v. *France*, No. 11801/85, 24 April 1990, §27, *Kopp* v. *Switzerland*, 13/1997/797/1000, 25 March 1998, §55.

[63] *Khan v. the United Kingdom,* No. 35394/97, 12 May 2000, §27.

However, the mere presence of law does not make the regime automatically "in accordance with the law", since the law itself must have the quality of law. This implies a number of requirements.

First, the law in question should not contravene other laws, in particular superior laws. For instance, the ECJ established that even provisions with a basis in European law may yet lack the qualities of law by contravening common European human rights standards and thereby may be contrary to common European law.[64] Examples include ECJ decisions finding that the EU Data Retention Directive[65] and the EU-USA "Safe Harbour" agreement on transferring personal data to the USA[66] both were in violation of the EU law.

Specifically, the Court ruled that the Data Retention Directive, which concerned all persons and required the retention of all means of electronic communication, exceeded the limits imposed by compliance with the principle of proportionality and was invalid.[67] The Court found that the "Safe Harbour" agreement was invalid,[68] despite the fact that the European Commission had earlier decided that the Safe Harbour regime was adequate. Not only the Snowden revelations of mass surveillance in the USA were grounds for the case: even before the revelations, various reports showed that the entire US data privacy framework was inadequate.[69]

Another example derives from the ECtHR, which found the discretionary powers of stop and search in the UK Terrorism Act 2000 to be a breach of ECHR Article 8, notwithstanding that it was provided for by a statutory measure, on the ground that the provision of Article 8 stipulating "in accordance with the law" was not met, in particular, due to wide framed powers of the police officer, which were "neither sufficiently circumscribed nor subject to adequate legal safeguards against abuse".[70]

This means that some other conditions must be satisfied too. Logically, if a measure in aviation security is authorized by law, but does not meet requirements of privacy and data protection law, and does not provide adequate safeguards, then the measure can be argued to be not in accordance with law.

Secondly, the law should be adequately accessible to the person concerned, and it should ensure that any interference is reasonably foreseeable to the person

[64] C-402/05 P and C-415/05, *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council and Commission*, 3 September 2008, §269.

[65] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

[66] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and frequently asked, related questions issued by the US Department of Commerce.

[67] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications, etc*., 8 April 2014, §§69 and 71. For comprehensive analysis of the decision, see Graver and Harborg. *Datalagring og menneskerettighetene* (2015).

[68] C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 Oct 2015, § 106.

[69] See Sect. 2.3.3.3.

[70] *Gillan and Quinton v. United Kingdom*, No. 4158/05, 12 Jan 2010, §87.

concerned, that is, formulated with sufficient precision to enable the individual to regulate his conduct.[71] As mentioned above, this overlaps with the requirements of transparency (see above).

The requirements of accessibility and foreseeability constitute an essential legal protection against arbitrariness when fundamental rights are being limited.[72] The ECtHR has held that protection against arbitrariness is even more important as regards surveillance measures,[73] which may be very relevant for aviation security.

At first sight, the accessibility requirement is quite clear: ordinary citizens must have access to the law. However, the question is whether such access to the law is provided in the event, for example, that a specific document is contained only in paid databases, or has restricted access only (see above), or otherwise the access to it is limited due to one of "accessibility barriers" such as language availability, secrecy, etc.[74] Of course, the most relevant limitation in aviation security is restricting information due to security needs (see above).

The foreseeability requirement can be problematic as well. The ECtHR acknowledged that the requirements of the Convention, with regard to foreseeability, "cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly".[75]

Nevertheless, the Court said that in a system applicable to citizens generally, "the law must be sufficiently clear in its terms to give… an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life".[76] Accordingly, since aviation security measures are applicable to citizens generally rather than in the context of police investigation, the requirement of foreseeability is valid.

Thirdly, a law must be specific, precise and clearly defined. These requirements derive from the Human Rights Committee[77] comments on wire-tapping[78] and from §8 of General Comment 16,[79] which specifies that even in cases of lawful interference

[71] *Ibid.* §76, *S. and Marper v. the United Kingdom*, No. 30562/04 and 30566/04, 4 Dec 2008, §§ 95 and 96.

[72] *Liberty and Others v. United Kingdom*, No. 58243/00, 1 July 2008, §69.

[73] *Klass and others v. Germany*, No. 5029/71, 6 September 1978.

[74] See Bing. *Rettslige kommunikasjonsprosesser: bidrag til en generell teori* (1982) pp. 234–235.

[75] *Malone v. The United Kingdom*, No. 8691/79, 2 Aug 1984, §67.

[76] *Leander v. Sweden,* No. 9248/81, 26 March 1987, §51.

[77] The UN Human Rights Committee is the body of independent experts who monitor implementation of the ICCPR by its State parties.

[78] ACLU. *Privacy Rights in the Digital Age*. March 2014. https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf

[79] General Comment 16, issued 23 March 1988 (UN Doc A/43/40, 181–183; UN Doc CCPR/C/21/Add.6; UN Doc HRI/GEN/1/Rev 1, 21–23).

with the right to privacy, "relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted". This approach can also be found in case law.

For instance, according to the ECtHR, in cases of telephone tapping, in order to make a surveillance measure lawful, national laws should define:

- categories of people liable to have their communications monitored;
- nature of the offences which may give rise to an interception order;
- limits on the duration of such monitoring;
- procedure to be followed for examining, using and storing the data obtained;
- precautions to be taken when communicating the data to other parties;
- circumstances in which data obtained may or must be erased or the tapes destroyed.[80]

However, these six requirements cannot be applicable generally, and should be applied on a case-by-case basis: e.g. the ECtHR distinguishes a greater degree of interference with privacy (such as wiretapping and surveillance of telecommunications) and a lower one (such as GPS surveillance), accordingly, the requirements for the first case will be stricter.[81]

The required details on the measure relate to such data protection principles as minimality, purpose limitation, etc. Thus, explicit laws aimed at specifying the measure's correspondence to these principles can be considered as a pre-condition to a measure being lawful. However, as mentioned above, different restrictions for security needs may apply.

"In accordance with law" also implies that the domestic law must contain a measure of legal protection against arbitrary interferences by public authorities with the human rights,[82] covering judicial dimension of this principle. In the context of privacy/data protection, "domestic law should provide appropriate sanctions and remedies in cases of breach of the provisions of domestic law"[83] enforcing the principles of privacy and data protection.

As noted above, it is quite unrealistic that an individual can challenge a security measure as such. If a person refuses to undergo a particular aviation security measure, he/she can be either subject to an alternative measure (if any) or be denied the right to fly. Of course, a person may exercise various protest actions, such as passive radical action (not flying at all); wearing sunglasses or hats in order not to be recognized by face recognition, destroying CCTV cameras, giving false personal data

[80] *Huvig v. France*, No. 11105/84, 24 April 1990, §34 and *Kruslin* v. *France*, No. 11801/85, 24 April 1990, §35, *Uzun v. Germany*, No. 35623/05, 2 September 2010, §65.

[81] Increasing Resilience in Surveillance Societies (IRISS) (2013) p. 34.

[82] *Gillan and Quinton v. United Kingdom*, No. 4158/05, 12 Jan 2010, §77, *Ollson* v. *Sweden*, No. 10465/83, 24 March 1988, §61.

[83] §7 of Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling adopted by the Committee of Ministers on 23 Nov 2010.

when booking. But, if wearing sunglasses, he/she may be targeted by security personnel and thereby be subject to even more measures; in the two latter cases, criminal liability may arise.

Typically, such protests and individual actions against the system are not very effective. The point is that those who carry out the security measures in practice have no interest or power in changing the system – they are not the ones who control the security system.[84] As Schneier notes, "The only way to change security is to step outside the system and negotiate with people in charge".[85] Helpful societal measures may include opinions and actions of opinion leaders, celebrities, activists (e.g. Edward Snowden's case), collective actions via specific groups, e.g. privacy advocates, demonstrations, counter-surveillance (watching the watchers), public opinion, etc.[86] As mentioned in Chap. 1, one of the most effective and practical roles in these processes is that played by data protection authorities, human rights organizations, privacy advocates etc., that is, groups who in some cases can influence the regimes.

In this section, judicial/administrative remedy refers to particular remedies for a person who believes he/she suffered in the result of existing procedures. In particular, if privacy/data protection invading technology is used by a security organ. Even if the measures are used according to the law and in compliance with the limitations allowed by human rights law, this organ's actions can be challenged before a judge or some other independent and impartial mechanism.[87]

Judicial protection is closely connected to the data subject influence principle (see below). For instance, data subjects should have a method available to them to hold data collectors accountable for following the data protection principles (DPD Articles 22–23).

This leads to a question: how to provide this legal protection against arbitrary interferences, where should air passengers apply if they believe that their privacy/data protection rights are violated in the course of security measures? This depends greatly on the national systems, which are supposed to establish concrete procedures, but typically, the following available mechanisms for privacy/data protection issues can be relevant: (i) airport or airport security department, airline, entity or law enforcement agency personnel who actually perform aviation security tasks (in data protection terms – controllers or processors); a usual method will be lodging of a complaint; (ii) national data protection authorities or other relevant supervisory organs; and (iii) courts. Chap. 7 will provide more details.

[84] Schneier (2008) p. 73.

[85] *Ibid.* p. 74.

[86] See Wright et al. (2015) p. 289.

[87] Aquilina (2010) p. 142.

5.3.1.4 Legitimate Aim

The "legitimate aim" criterion is connected to both the general legality principle and the data protection's purpose limitation principle. In general, surveillance can be permitted by laws only if it contributes to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.[88] The aviation security measure must be in pursuit of one of the aims set out under ECHR Article 8(2).

As discussed in Chap. 4, aviation security measures are carried out to safeguard civil aviation against acts of unlawful interference – more broadly, in the interests of national security, hence falling within Article 8(2). Thus it seems it is quite easy for the aviation security measures to satisfy the "legitimate aim" criteria. The problem is that such objective may be very wide in scope. Since it is the state that identifies the objective(s) of the interference, it can usually make "a plausible case in support of the interference".[89]

It may occur that the reason given by the state is not the "real" reason motivating the interference, with other reasons and motivations behind, but in most cases, the court will still accept that states are acting for legitimate purpose.[90] The main idea is that terrorist offences and serious crimes constitute threats to other fundamental rights, especially the right to life; thus, their prevention, detection, investigation and prosecution are also legitimate in order to protect the rights and freedoms of others.

In this case, the overlapping data protection principle – purpose limitation – can contribute to defining "legitimate aim" since it requires that the goal should be set clearly and be purpose specific (see below).

5.3.1.5 Lawful Processing

Furthermore, the principle of fair and lawful processing is a primary principle for data protection law stipulated in DPD Art. 6(1)(a). "Lawful processing" can be defined from the discussion above: in general, this means that any processing should have legal grounds and should be carried out according to the law, i.e. satisfying all other data protection requirements as well. DPD Article 7 stipulates criteria for making a data processing legitimate: if the controller pursues a legitimate aim (§§e-f); if the data subject has given his unambiguous consent (§a).[91] In the UK Information Commissioner's guide to data protection, one of the conditions for

[88] International Principles on the Application of Human Rights to Communications Surveillance, signed by 258 non-governmental organizations. Final version 10 July 2013. https://en.necessary-andproportionate.org/text

[89] Kilkelly (2001) p. 30.

[90] *Ibid.*

[91] Gutwirth [et al.] *Deliverable D1: legal, social, economic and ethical conceptualisations of privacy and data protection* (2011) p. 27.

lawful processing of data is to "make sure you do not do anything unlawful with the data"[92] implying that other data protection principles should be respected.

Moreover, if national data protection legislation is absent, some endeavours should be made by the states to establish procedures, develop laws or rules for protection of personal data process by security measure in question.[93] This means that requirements to the law concern not only the laws on aviation security measures, but the laws on specific data protection as well.

5.3.1.6 Concluding Remarks

It is clear that the legality principle should be applied on a case-by-case basis. But in general, pursuant to the legality principle, aviation security measures should serve legitimate aims, have a legal basis in law which respects other laws and is accessible to the citizens, who must be able to foresee the consequences with regard to privacy interference, the law must contain judicial protection against arbitrary interferences, and processing of personal data should be lawful. However, due to the specific nature of aviation security, with a substantial volume of restricted information and the possibility of restriction due to security needs, some particular requirements can be difficult if not impossible to fulfil. At the same time, as indicated above, any exceptions and restrictions must be provided by law, be necessary and proportionate.

5.3.2 Proportionality Principle

5.3.2.1 Introduction

The proportionality principle is particularly important for this research and its results, since it is the key instrument for analysing aviation security versus privacy dilemma. As mentioned in the Introduction, a close term which is used extensively with respect to the dilemma and sometimes is confusing with proportionality is "balancing". Here, a more detailed analysis of these terms will be presented.

In addition, the proportionality principle is relevant for privacy and data protection and for aviation security. As discussed in Chap. 4, security solutions should be proportionate to the probability of the threat and possible harms, costs and benefits, etc. Obviously, the concrete set of factors to be taken for assessing proportionality within the aviation security will differ from those used within privacy/data protection; however, there are some overlapping factors.

---

[92] ICO. Guide to data protection. https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/

[93] See, e.g. ICAO PNR Guidelines, §2.12.

While effectiveness was discussed in Chap. 4, here, the proportionality principle in privacy/data protection will be developed in more detail below to indicate how this principle will be further used in the Special Part.

5.3.2.2 Balancing

With reference to "security versus privacy", a common suggestion is the idea of finding the balance between these values, in other words, to balance privacy (or, broadly, liberty) against security using the so-called trade-off model. According to the latter, it is not possible to increase one of the values without decreasing the other one: "respecting civil liberties often has real costs in the form of reduced security" and vice versa.[94] The key issue here is optimization: to choose the point that maximizes the joint benefits of security and liberty.[95]

The term "balance" is undefined in these theories. But generally, this word has a number of meanings, with some of them applicable here. The first one is "a state of equilibrium or equipoise; equal distribution of weight, amount, etc".[96] In the philosophical context, balance is used to mean "a point between two opposite forces that is desirable over purely one state or the other".[97] Aristotle and other philosophers called this point "the golden mean" (i.e. the middle ground between extremes) and applied it to ethics or politics.

Another meaning of "balance" is an "instrument for comparing the weights of two bodies, usually for scientific purposes, to determine the difference in mass (or weight)".[98] As Waldron states, balance "has connotations of quantity and precision".[99] Apparently, this can be relevant to trade-offs between security and privacy or any other conflicting interests. Consequently, within these two meanings of the term "balance", balancing is aimed to find the golden mean for the privacy and security, and at the same time, can "measure" both ends (although the problem of measuring intangible values remains).

The balancing idea can be found in the ECtHR case law, stating that "inherent in the whole of the Convention [ECHR] is a search for a fair balance between the demands of the general interest of the community and the requirements of the protection of the individual's fundamental rights".[100] Therefore, the rights of the individual can be balanced with the interests of the state.[101]

---

[94] Posner and Vermeule (2007) p. 32. See also Vermeule. *Security and Liberty: Critiques of the Tradeoff Thesis*. In: Harvard Law School Public Law & Legal Theory Working Paper Series (2011).

[95] *Ibid.* pp. 26–27.

[96] Dictionary.com. http://dictionary.reference.com/browse/balance

[97] Wikipedia. http://en.wikipedia.org/wiki/Balance_(metaphysics)

[98] Encyclopedia Britannica. http://www.britannica.com/search?query=balance

[99] Waldron (2003) p. 192.

[100] *Soering v. the United Kingdom*, No. 14038/88, 7 July 1989, §89.

[101] Kilkelly (2001) p. 31.

In aviation security, balancing is important too. First, it can be stipulated by law, as in Russian Law on transport security, where "balancing the interests of the individual, society and the state" is one of basic principles of transport security.[102] The issues of threats and risks and effectiveness of aviation security discussed in Chap. 4 are generally used to explain the need for balancing and trade-offs with compromising the human rights in the name of security.

In addition, since the threat to security constantly grows, the balance is supposed to be changed accordingly. For instance, terrorist incidents in the 1970s had maximum death tolls of about a dozen; attacks in the 1980s and 1990s – hundreds; 9/11 – thousands; today, weapons of mass destruction may kill hundreds of thousands – therefore, "As risks change, we who care about civil liberties need to realign balances between security and freedom. It is a wrenching, odious task, but we liberals need to learn from 9/11 just as much as the FBI does".[103]

It looks like a change in the scale of the threats, especially after 9/11, justifies a change in the scheme of civil liberties. Accordingly, the weight of security is growing while the weight of privacy is sinking, leading to a more vertical new balance line. This process is often described as "striking a new balance between liberty and security",[104] leading to compromises in the name of security. Hence, any limitations or violations of human rights and freedoms that may have seemed disproportionate, unnecessary and unreasonable before 9/11 may now be deemed proportional, necessary and reasonable respectively.

The concept of the balance and trade-off model is subject to criticism first of all because it justifies such compromises, with the right to privacy being one of the first "victims of a balancing approach".[105] Two types of critics can be distinguished: internal and external.[106]

"Internal" critics object to the way in which trade-offs are evaluated and judged, claiming that the balance is always skewed in favour of security, at the expense of the right to privacy, leading to a systematic erosion of civil liberties in the name of security.[107] Some argue that accepting that the weight of some human rights depends on circumstance makes human rights principles inconstant, and the process of balancing can possibly "swallow up the rights".[108] The ECtHR issued a reminder that although measures which interfere with privacy may be designed to protect democracy, they should not destroy it in the process.[109]

---

[102] RF Federal law of 9 February 2007 N 16-FZ On transport security, Art. 3(2).

[103] Waldron (2003) p. 192 citing Kristoff. *Liberal reality check: we must look anew at freedom vs. security*. In: Pittsburgh Post-Gazette (2002) p. A9.

[104] *Ibid.*

[105] Scheinin and Vermeulen (2011) p. 49.

[106] Amicelli (2012a) p. 13.

[107] *Ibid.*

[108] Cali. *Balancing Human Rights? Methodological Problems with Weights, Scales and Proportions*. In: Human Rights Quarterly. Vol. 29 (2007) p. 253.

[109] *Malone v. The United Kingdom*, No. 8691/79, 2 Aug 1984, §82.

But, it is noteworthy that even juridical review can be of little help, since it runs the risk of accepting too many compromises in the name of balancing: "If such a court in normal times lets itself be strongly "pulled" into the approach of balancing, it may be unable to break loose of the frame when the day comes when it should".[110] It is also claimed that the process of balancing "tangible values against intangible harms" presents the debate from the view that privacy is "a mere abstraction, a luxury with little concrete value".[111] Internal critics, nevertheless, offer no objection to the security-privacy balance and often acknowledge that trade-offs are necessary.[112]

"External" critics may deny first the whole trade-off model. But, such denial may be discarded here: apparently, no matter how you describe or interpret the security and privacy dilemma, it is not possible today to avoid balancing and, accordingly, the concepts of balance and trade-off. Any stakeholders may take part in the balancing process. Trade-offs in practice at the airports can be seen from multiple perspectives. If the trade-off is evaluated from the air passengers' view, in exchange to the ability to fly, they have to perform certain actions, including going through the security checks and complying with security rules. From the view of the aviation industry, commercial airlines, the trade-off is made for the possibility of conducting business operations. However, if the security measures place an unacceptable burden and may substantially infringe on business, they might be unacceptable. Regulation of security procedures and their implementation have certainly invoked some trade-offs, but it is up to the decision-makers to establish the final balance, where the interests and convenience of passengers, for example, may be considered as less important than the security effectiveness issues. Thus, in this research, it is presumed that balancing and trade-offs do exist.

Secondly, external critics deny that the issues of security and privacy are best thought of in terms of balancing or trading off of one for the other.[113] For instance, within aviation security, threats, risks, effectiveness and other factors are used to balance aviation security needs with human rights and compromise the latter in the name of security. The problem is that it is difficult to define the trade-offs sufficiently enough to get a clear sense of how much security is bought for how much cost: it is impossible to say with confidence that e.g. this particular aviation security measure reduces by X percent the chance of a bomb getting on board; instead, the avoidance of terrorist attacks is treated as an absolute goal.[114] Clearly, the aviation security agencies' interests and motivations are not same as those of the population as a whole: e.g. their biggest interest is not in finding the public's preferences about where to find the balance, but in avoiding a terrorist attack: for instance, if an attack

[110] Scheinin. *Terrorism and the "Pull" of Balancing in the name of security* In: Law and Security: facing the dilemmas (2009) p. 57.

[111] Spencer (2002) p. 519.

[112] Amicelli (2012a) p. 13.

[113] *Ibid.*

[114] Pillar. *The Price of Aviation Security.* The National Interest. 22 November 2010. http://nationalinterest.org/node/4463

occurs, few will defend the responsible aviation security agency that it was operating according to public privacy preferences; instead, the agency will be blamed that it failed to do its job to determine what was necessary to stop the attack.[115] Thus, the result of any balancing is always definite.

Clearly, the security versus privacy dilemma is "much more complex, nuanced and subtle than suggested by the trade-off model".[116] According to this critical view, the processes of finding a "balance", trading civil liberties for security are not only unnecessary, but may also be dangerous. The critics urge caution about giving up civil liberties/privacy for the sake of security and refer to Franklin's famous: "they that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety".[117] Schneier, expressing scepticism towards all security measures (apart from those above that cause no negative impact on privacy) and calling them "security theatre," adds that "We are not trading privacy for security; we are giving up privacy and getting no security in return".[118]

Accordingly, the privacy-security dialectic approach was formulated, seeing a positive relationship between privacy and security: "Security and privacy are not opposite ends of a seesaw; you don't have to accept less of one to get more of the other;"[119] "Liberty cannot be enjoyed without security, and security is not worth enjoying without liberty;"[120] liberty requires security without intrusion, i.e. security plus privacy, and there is no security without privacy[121]; privacy can be protected without cost to security,[122] etc. As Raab notes, this approach may strengthen the management of security and keep it within a society that values equality and freedom.[123] For this approach, the use of the proportionality principle discussed below can be helpful.

5.3.2.3 Proportionality Principle, in Particular in Privacy/Data Protection

The general principle of proportionality is a worldwide legal principle, a key organizing principle of legal thought.[124] It is found in both the common and civil law, bringing them together to a global uniform jus commune; it is found before national

[115] Pillar (2010).

[116] Amicelli (2012a) p. 14.

[117] Franklin. *Memoirs of the life and writings of Benjamin Franklin* (1818). Available also in: Benjamin Franklin, Historical Review of Pennsylvania, 1759? John Bartlett (1820–1905). Familiar Quotations, 10th ed. 1919.

[118] Schneier (2008) p. 9.

[119] *Ibid.* p. 69.

[120] Vermeule (2011) p. 26.

[121] Schneier (2008) p. 70.

[122] Solove (2011) p. 3.

[123] Raab. *Privacy as a Security Value*. In: Jon Bing: En Hyllest/A Tribute (2014) p. 58.

[124] Engle. *The History of the General Principle of Proportionality: An Overview* (7 July 2009). In: Dartmouth Law Journal, Vol. X-1 (2012) p. 3.

and transnational courts.[125] It is enshrined in international/EU/national legal instruments with reference to different areas.[126]

In Europe, the test of proportionality is the most acknowledged method of legal evaluation of conflicts of fundamental rights and legitimate interests, such as privacy and security.[127] It is relatively closely tied to people's concrete non-legal world experiences: it only requires a comparison of two countervailing factors.[128]

At the same time, the need of such "comparison" reveals that there is a close connection between the balancing and proportionality principle, and in the ultimate scenario, the proportionality principle in practice can easily turn to balancing. This allowed some researchers to differ "weak" and "strong" proportionality tests, with the weak one amounting to balancing privacy and security, presuming that the one per se weakens the other and excluding the possibility that both interests can co-exist together.[129]

In contrast to that, the key point within a strong proportionality test – hereinafter referred in this work to as "proportionality principle" – is that the simple fact that technologies are available, affordable or are believed to get public approval does not constitute sufficient reason for them to be used.[130] As mentioned in Chap. 1, in aviation security, there is a tendency that if new technologies enhance security, they should be used as soon as they are available, but from a privacy/data protection perspective, any contribution to security in itself is not a justification: the availability of means should not justify the end.[131]

The key idea is that the limitations on the rights of individuals by technology should be proportionate to the expected security benefits. In other words, the restriction on privacy/data protection should fulfil its purpose, and there has to be concrete evidence that there is genuine threat to public security and this is an appropriate way of responding.[132]

Even though a security measure contributes to security, such a measure may be unacceptable if it harms privacy to an excessive degree. Thus, instead of balancing, where it is accepted that privacy is outweighed by security, it is important to answer how much harm to a human right would be tolerable in a democratic state in which human rights are protected.[133] It is proposed that the language of rights – not the

---

[125] *Ibid.*

[126] E.g. it applies under public international law, private international law, public and private domestic law. With applicability to the EU institutions, the principle of proportionality is laid down in Article 5 of the Treaty on EU.

[127] Wright et al. (2015) p. 288.

[128] Cankorel (2008) p. 180.

[129] Gutwirth et al. (2011) p. 27.

[130] Information Commissioner's Office (2014) and Lyon (2004) p. 142.

[131] European Data Protection Supervisor. *Opinion on the Communication from the Commission on the global approach to transfers of Passenger Name Record (PNR) data to third countries* (2010).

[132] Colvin. *The Human Rights Act and CCTV*, CCTV User Group, 12 October 2007, https://www.cctvusergroup.com/art.php?art=39

[133] Gutwirth et al. (2011) p. 27.

language of balance should be used.[134] In other words, first, a presumptive weight to the right to privacy should be given, and then, the limitations to the right in a narrow manner should be construed.[135]

The point, as discussed in Chap. 3, is that human rights law provides lawful grounds for derogations, restrictions and limitations if they serve definite purposes: to protect national security, public order, public health or morals or the rights and freedoms of others. Having these existing norms – *lex lata* – as a point of departure, in respect of *lex ferenda,* it can be noted that from being only *subject* to balancing and the trade-off model, human rights should move to another dimension. Specifically, they should regulate the balancing process as such, via applying the test of limitations and the proportionality test in that process.[136]

The CFREU Article 52 provides explicitly that "[s]ubject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others". This refers to criteria and legitimate aim discussed above, as well as necessity, which will be discussed below. However, a mechanism for the application of the proportionality principle is missing.

In contrast to privacy, processing of personal data is not framed as an interference with a right (cf. ECHR Article 8(2)). DPD Articles 6(c) ("relevance", "not excessive"), 7, 8 and 13 ("necessary") manifest the proportionality principle. Altogether, this means that even when the aims of data processing are legitimate according to Article 7, they will only be legitimate if the data collection and processing correspond to the needs for realizing a specified purpose and are proportional, i.e., necessary, adequate, relevant and not excessive; moreover, if the specified purpose can be reached without personal data processing or by processing less personal data, than the processing can be considered as disproportionate and thus illegitimate.[137] However, the DPD, although establishing these requirements, does not contain any further explanations on what "proportional", "necessary", and other terms imply.

Thus, it is difficult to assess criteria of proportionality objectively. In addition, the methods and criteria of the proportionality test vary from jurisdiction to jurisdiction, from court to court and from case to case.[138] In this research, criteria will be addressed taking into account the views of the ECtHR and the ECJ, as well as data protection authorities and research literature.

The case law, in particular the practice of the ECJ[139] and the ECtHR, increasingly recognize the proportionality principle for both privacy and data protection, for the latter, as a core data protection principle in its own right.[140] The strict methodology

---

[134] Walker (2006).

[135] Gallagher (2002) p. 288.

[136] Scheinin and Vermeulen (2011) p. 50.

[137] Gutwirth et al. (2011) p. 28.

[138] *Ibid.* p. 26.

[139] C-465/00, *Rechnungshof* decision, 20 May 2003, § 91.

[140] See, for example, Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 Nov 2010.

of the proportionality test is used when the courts make decisions on the justifiability of concrete cases of restricting fundamental rights, such as the application of surveillance measures. If the legitimacy of surveillance is questioned, the dispute in most cases is resolved by courts, applying the test of proportionality.[141]

The case law has developed specific criteria to assess whether a surveillance measure can be considered proportionate. For the purposes of this research, the criteria can be combined into several groups.

First, the proportionality principle requires that the grounds for the security measure's interference must be sufficiently important to limit the right,[142] in other words, the interference must meet "a pressing social need".[143] Accordingly, the aviation security measure must be suitable (appropriate, relevant, adequate) to fulfil the specific legitimate aim. Hence, two important issues should be considered in combination: legitimate aim and the measure's suitability.

As for legitimate aim, as mentioned above, it should be set clearly and be purpose-specific. In particular, it should specify the specific harm that a measure is intended to prevent/detect. Thus, purpose limitation principle should be applied, since understanding of the purpose helps to determine additional criteria for the measure to be proportionate: the categories or types of data needed, the type of processing, the quality of the data, etc.[144]

Determination of suitability of aviation security measures depends greatly on the factors discussed in Chap. 4, where security decisions are aimed to determine appropriate and most effective security measures taking into account threats, risks, possible harms, costs, benefits, etc. Possible harm if the measure is not provided at all can also be taken into account. The key element for fulfilling the legitimate aim is effectiveness, which implies that the measure concerned must be effective in achieving its specific purpose.

The second criterion is necessity – the measure concerned must be necessary to realizing these goals.[145] In some cases, a more stringent standard is applied – in order to be necessary, the measure should be indispensable. According to the ECJ, in order for security measure be proportionate, it has to be demonstrated that other less intrusive methods are not available.[146] If there is a choice between several appropriate measures, recourse must be used to the least onerous.[147] Accordingly,

[141] Wright et al. (2015) p. 288.

[142] Fordham and De La Mare. *Identifying the Principles of Proportionality.* In: Understanding Human Rights Principles, London: Justice and Hart Publishing (2001).

[143] Spielmann. *Allowing the Right Margin the European Court of Human Rights and the National Margin of Appreciation Doctrine: Waiver or Subsidiarity of European Review?* In: Centre for European Legal Studies, Working Paper Series (2012) p. 22.

[144] Article 29 Data Protection Working Party (2014a).

[145] Case C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, 16 December 2008, § 66.

[146] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 Nov 2010, §§ 81 and 86.

[147] Case T-13/99, *Pfizer Animal Health SA* v. *Council of the European Union*, 11 Sept 2002, §12.

taking into account reasonable costs, if there are other aviation security measures which are less intrusive or non-intrusive and capable of providing equal security, i.e. to achieve same purpose with the same result, this least harmful choice should be used.

Therefore, before adopting any new measure, existing measures and alternatives should be assessed, including effectiveness issues and evidence on why existing measures are not sufficient; it should be explained whether other measures were found to be more or less privacy-intrusive; if those which were found to be less intrusive were rejected, this should be justified.[148] As discussed in Chap. 4, it is possible to increase security at no cost to privacy, e.g. via reinforcing cockpit doors, in-flight security officers, and training crew and passengers. The problem is that neutral measures probably cannot substitute all other measures which are used or are planned to be used.

Thirdly, as formulated in case law, the measures "should not exceed the limits of what is appropriate and necessary in order to attain the legitimate objectives".[149] This is criteria of non-excessiveness: the measure must not go further than is necessary to realize the goals.[150] As discussed in Chap. 3, excessiveness may refer to both the form of particular measures and the manner of executing them. It depends greatly on concrete circumstances of a particular situation: the measure may be deemed to be non-excessive despite inconveniences such as loss of privacy caused by this measure.

But if a measure is nevertheless used, its scope must be limited to the absolute minimum. For instance, such elements as the number of people affected by the aviation security measure, the amount of personal data collected, how long it is retained, who has access to it, may often be excessive,[151] and enhancing these options must be done only with due cause. In order to minimize the excessiveness, different safeguards can be helpful and should be used, e.g. organizational or technical means to limit the scope of the measure. Here, an overlap with the minimality principle of data protection discussed below can be noted.

Simply said, in respect to every separate aviation security measure, it is necessary to answer the questions: how good the measure is to actually provide security and to justify privacy concerns, and whether everything possible is done to minimize the latter. The relationships can be illustrated like this:

As shown in Fig. 5.1, privacy risks here should strive towards the minimum, while security advantages should strive towards the maximum, ideally, with zero privacy risks and maximum security benefits indicated as (1). The diagonal blue line indicates rough borders between "proportionate" and "disproportionate" zones. If privacy risks are high, but security benefits are low, the measure cannot be considered proportionate (2). In addition, certain limitation to allowed maximum risks to privacy should be determined too (red line). Apparently, (3) and (4) can be seen as

[148] Article 29 Data Protection Working Party (2014a).

[149] *Pfizer Animal Health SA* v. *Council of the European Union*, §12.

[150] Fordham and De La Mare (2001).

[151] Article 29 Data Protection Working Party (2014a).

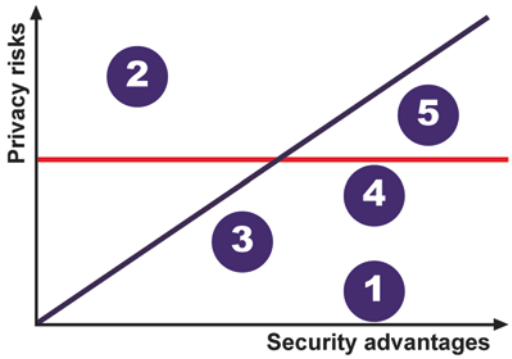

Fig. 5.1 Proportionality principle applied to privacy and security

proportionate, if privacy risks are lower than security benefits and do not go beyond the red line. If risks exceed this allowed maximum (5), no matter which security benefits can be expected, this measure cannot be considered appropriate. An absurd example is naked passengers on board.

The problem that emerges is that it is impossible to determine the risks of privacy and security advantages or the golden middle point mathematically and place them on the figure exactly. While some extreme examples are quite easy to judge, such as metal detectors or cockpit doors without privacy concerns, many measures appear somewhere in the middle.

Thus, within this approach, assessment of what is proportionate must be ascertained on a case-by-case basis, and many different factors should be taken into account. In particular, all circumstances of the case, including the context and nature of the interference, scope and duration of the measure, the type of information collected (sensitive or not), relevant authorities permitting, carrying out and supervising the measures, and remedy provided by the national law,[152] provision of safeguards, etc. For example, the privacy considerations in terms of context are very different for CCTV cameras in public zones or in toilets at the airport or aircraft.

Broadly, the need to analyse many different factors means that any possible concerns related to other privacy and data protection principles – and even more broadly, to other applicable human rights discussed in Chap. 3 should be taken into account when assessing proportionality of the measure. This approach confirms the idea that the all the principles and all the human rights should be considered together, since concerns associated with any of them may have influence on the aggregated impact of the security measure.

It is commonly accepted that it is to the state's obligation to justify the interference. On the one hand, the more severe the interference and the more intrusive the technology, the more approvals and the stronger the reasons required to justify it.[153]

[152] See, e.g. *Klass and others v. Germany*, No. 5029/71, 6 Sept 1978, §50, *Malone v. the United Kingdom*, §§66–68, *Liberty and other organisations v. the United Kingdom*, No. 58234/00, 1 July 2008, §§93–94.

[153] Kilkelly (2001) p. 32 and Aquilina (2010) p. 14.

Since aviation security measures are mainly preventive measures, and are carried out without a concrete and individualized law enforcement context, this requires even more substantiation of the measure. On the other hand, the more severe the issue and more substantial the harm which society may be exposed to, the more interference may be justified.[154]

In aviation security, as discussed in Chap. 4, the risks of terrorism and crime and the consequent harms are considered as enhanced, thus, the non-deployment of security measures would be deemed inadequate, and the aviation security measures seem to be easier to justify than those seeking to protect, for instance, morals.[155] At the same time, if the technologies imply serious harms to privacy, they require justification.

Thus, in aviation security, despite the possible harms, justification is required, in particular, if impact on privacy is serious, and it is the state that should prove the suitability of the aviation security measures, their non-excessiveness, necessity, as well as correspondence to other criteria.

However, in determining whether a particular measure is compatible with ECHR Article 8 the state, when identifying their pressing social need and the level of interference when pursing a legitimate aim, has a certain degree of discretion, or a margin of appreciation. It means a freedom to act, or the latitude of defence or error which the Strasburg organs will allow to national bodies before it is prepared to declare a national derogation from the ECHR, or restriction or limitation upon a right guaranteed by the ECHR, to constitute a violation of the ECHR.[156] According to the Court, margin of appreciation must be derived from "a just balance between the protection of the general interest of the community and the respect due to fundamental human rights while attaching particular importance to the latter".[157]

According to this doctrine, domestic authorities are best to settle a dispute.[158] Since security falls within a valid aim within Article 8(2), a margin of appreciation granted to the state is wide.[159] Nevertheless, the states do not get an unlimited power of appreciation and it is the ECtHR who gives the final ruling on whether interference can be justified under Article 8 (2). But, according to some researchers, if distinguishing between weak and strong proportionality tests discussed above, the

[154] Article 29 Data Protection Working Party (2014a).

[155] Kilkelly (2001) p. 32.

[156] Yourow. *The margin of appreciation doctrine in the dynamics of European human rights jurisprudence* (1996) p. 13.

[157] Case *"Relating to certain aspects of the laws on the use of languages in education in Belgium" v. Belgium*, No 1474/62; 1677/62; 1691/62; 1769/63; 1994/63; 2126/64, 23 July 1968, §5. See also e.g. *Lingens* v. *Austria*, No. 9815/82, 8 July 1986, §39.

[158] Spielmann (2012) p. 2.

[159] *Ibid.* pp. 14, 16. For example, in *Leader v. Sweden*, the court did not find violation of Article 8 because the applicant was regarded as a national security risk. *Leander v. Sweden,* No. 9248/81, 26 March 1987, §59.

Court acknowledges the need to take effective measures against crime and terrorism, but applies a weak version of the proportionality test or avoids it.[160]

The margin of appreciation doctrine has a number of other weaknesses: a degree of vagueness, a risk of manipulation of the identified factors and parameters, and lack of legal certainty.[161] Despite the core of the legal balancing between privacy and security lies in the proportionality and "necessary in a democratic society" tests (and the parameter of proportionality offers more legal certainty[162]), in many privacy cases the courts put the emphasis on the legality test.[163] This means that if the aviation security measure has a basis in law, this will be more valued than the proportionality/necessity considerations.

Consequently, it is argued that the proportionality principle is more a mediatory principle, which is "effective in questioning means of action, but silent on the ends of the action".[164] Thus it helps to judge, but can hardly provide a clear and concrete decision.

At the same time, with reference to recent ECJ jurisprudence in the data privacy field, the court is increasingly applying the proportionality principle in a stringent way. Examples include the *Schrems* case, where the ECJ found that the "Safe Harbour" agreement on transferring personal data to the USA is invalid.[165] In particular, it was noted that the US authorities were able to access and process personal data transferred from the EU to the USA under Safe Harbour beyond what was strictly necessary and proportionate to the protection of national security (§90).

In *Google Spain*, by virtue of the principle of proportionality, it was held that the operator of a search engine is responsible for the processing that it carries out of personal information which appears on web pages published by third parties.[166] In *SABAM,* the ECJ found that imposing a general filtering obligation on Internet service provider does not respect the requirement of proportionality.[167] All these rulings resulted in concrete decisions, with direct consequences for the respective situations or regimes.

---

[160] Gutwirth et al. (2011) p. 26.

[161] Lester. *The European Court of Human Rights after 50 years*. In: European Human Rights Law Review. Vol. 4 (2009). p. 474, Spielmann (2012) p. 28.

[162] Arai-Takahashi. *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR* (2002) p. 14.

[163] Gutwirth et al. (2011) p. 27.

[164] Cali (2007) p. 270.

[165] Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 Oct 2015, § 106.

[166] Case C-131/12, *Google Spain SL, Google Inc. V. Agencia Española de Protección de Datos, Mario Costeja González*, 13 May 2014, §§ 63 and 3.

[167] Case C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011, § 53.

5.3.2.4 Concluding Remarks

The proportionality principle is the key principle for this research. Moreover, it seems to be increasing in importance: it is proposed, for example, that the methodology of proportionality principle should be used at the level of planning, introducing or increasing aviation security measures.[168] Regulatory or self-regulatory measures should be taken in order to encourage or oblige the interested parties, formally and substantially to apply this methodology.[169]

Within the proportionality principle, the general rule is: if an aviation security measure implies an intrusive act that interferes with the rights to privacy and data protection, decisions about it must be made by weighing the benefit sought to be achieved against the harm that would be caused to the rights. The compromise has to be proportionate to the threat perceived and the benefits of the use of that concrete aviation security measure.

As discussed, although taking into account passenger experience is increasing, it is still not so common for the aviation security to evaluate possible harms to privacy and data protection *before* enforcing a particular aviation security measure. Frequently they are considered post-factum.

Accordingly, two processes which both use proportionality tests can be noted: (i) evaluating by security providers which security solutions to implement, according to threats and risks, costs and benefits, and (ii) evaluating whether the privacy/data protection risks are proportionate to the benefits of the measure, which, by the way, takes into account all the conclusions of the first one.

As a rule, these are two separate processes, with different aims. They do not necessary run parallel – the second one may be conducted after the first one, sometimes with a period of time between the two. For instance, the installation of body scanners in some airports took place much earlier than the decision-makers started to participate in public discussions about privacy concerns, e.g. in the USA and the UK. However, in some cases, privacy concerns raised *before* the implementation of a measure may cancel or postpone it until the concerns are solved.[170]

Another problem is that the first process is carried out by the relevant national authorities in secret; as a rule, the processes of threats and risks assessments and their results are not open to public. Thus, they are outside the scope of democratic debate – a proper, democratically accountable way of making aviation security decisions is missing.

Taking into account all these factors, in general, it can be concluded that what is proportionate for the aviation security is not always proportionate for privacy/data protection. At the same time, the overlap exists, since the suitability (effectiveness) and necessity may have direct effect on both aviation security and privacy/data protection considerations. Moreover, aviation security, as discussed, slowly but surely

[168] Wright et al. (2015) p. 288.

[169] *Ibid.*

[170] As in the case of body scanners in Norway, which testing was cancelled due to privacy concerns in 2007. However, in 2015, framework contracts for scanners were concluded, see Chap. 6.

takes into account privacy/data protection considerations both as the cost of security solutions and as benefits – the means to improve passenger experience. In some cases, privacy risks may freeze or cancel even promising in security terms measure. In other cases, enhancing privacy may contribute to passenger experience.

Accordingly, the proportionality principle is indeed the key principle for this research, and will be extremely helpful for the security-versus-privacy discussion. In the Special Part, to evaluate the proportionality of a concrete aviation security measure in privacy/data protection terms, the proportionality principle will be applied using the following scheme:

1. Suitability – is the aviation security measure suitable to fulfil the specific legitimate aim? The key element here is effectiveness, which implies that the measure concerned must be effective in achieving its intended purpose.
2. Necessity – is the measure in question necessary to realizing these goals, or are there other aviation security measures which are less intrusive but capable of achieving same result?
3. Non-excessiveness – does the measure go further than is necessary to realize the goals?

In addition, in order to assess whether a particular measure is proportionate, it is necessary to evaluate many other factors, including the severity of the interference, the sensitivity of the practice or data collected, and other contextual factors. Above all, it is necessary to assess the measure's compliance with other legal principles of privacy and data protection, its impact of other human rights, in order to determine the aggregated impact and compare it with the measure's security benefits. This will be done in the Special Part.

5.4 Principles of Data Protection

Similar to other legal principles discussed in this chapter, principles of data protection comprise the essence, nature and roles of principles discussed above and are contained in law. Data protection principles are also often called "standards", "requirements" and can be defined as "the basic principles applied by data privacy laws to the processing of personal data".[171] The core idea is that all the principles must be satisfied: complying with one of them does not exempt you from complying with the others; if the principles are understood, the whole data protection law will fall into place.[172] Accordingly, if all of them are applied to aviation security measures, they will allow to establish whether collection, storage, share, transfer, analysis or any other type of processing of personal data for aviation security purposes correspond to the requirements of data protection law.

[171] Bygrave (2014) p. 145.

[172] Information Commissioner's Office. The Eight Data Protection Principles. http://www.belb.org.uk/downloads/foi_data_principles.pdf

The principles of data protection are international – they are formulated in the DPD, Convention 108, OECD guidelines, etc. However, the principles contained in the EU law are the most influential internationally – they have legal weight beyond the EU – and there are jurisprudence and academic works clarifying them.[173] It is clear that they may be effective outside the EU jurisdiction repeated by laws of non-EU states, where data protection law was greatly influenced by the EU regime (see Chap. 2). In the aviation security and privacy context, these principles are fully or partly repeated by e.g. ICAO in its recommendations concerning PNR usage by the states, by EU and national data protection authorities giving guidelines on the use of biometrics, body scanners, CCTV, profiling, etc.

However, although principles of data protection are international, they are not global thus they lack the universal status of the international general principles, e.g. they do not apply on the territories which do not have data protection law as such.

For instance, while the USA assigns data protection principles a significant role in its regulatory regime, the principles are formulated differently (there are similar categories known as "the principles of fair information practices"[174]) and are applied less extensively than data protection principles in Europe. Some of the principles are reflected in the Privacy Act[175] and other sector-specific laws, however, these laws contain many exceptions so that important provisions are not applicable to the use of personal data on counterterrorism purposes, by law enforcement and intelligence agencies.[176] While general protection of commercial data in the USA is lacking, the principles of fair information practices provide a good starting point for governmental use of commercial databases.[177] Despite certain similarities in comparison with the EU data protection principles, it cannot be stated that the latter apply in the USA.

Moreover, there are variations in formulation and application of concrete data protection principles from instrument to instrument, from state to state, etc. which may also contribute to non-harmonization and divergences. For instance, there are differences between the provisions of the DPD, Convention 108, and provisions of more specific instruments with different legal status providing further details on concrete data processing technology or practice. Since the principles expressed in the DPD are "the most widely implemented privacy principles globally"[178] and keeping in mind the leading role of the DPD, this research will use the latter as the main source of the data protection principles.

Another issue is that even when using the DPD as the point of departure, there are divergences in interpretations and formulations of particular principles. Bygrave, for instance, indicates the following "core principles of data privacy law":

---

[173] Bygrave (2014) p. 146.

[174] See Dempsey and Flint. *Commercial data and national security*. In: Geo. Wash. L. Rev. Vol. 72 (2004) p. 1489.

[175] Privacy Act of 1974, 5 U.S.C. § 552a (2000).

[176] Dempsey and Flint (2004) p. 1489.

[177] *Ibid.* p. 1495.

[178] Greenleaf. *Five years of the APEC Privacy Framework: Failure or promise?* In: Computer Law & Security Report. Vol. 25 (2009). p. 32.

1. Fair and lawful processing
2. Proportionality
3. Minimality
4. Purpose limitation
5. Data subject influence
6. Data quality
7. Data security
8. Sensitivity[179]

Schedule 1 to the UK Data Protection Act lists the following eight principles:

1. Fairly and lawfully processed
2. Processed for limited purposes and not in any manner incompatible with those purposes
3. Adequate, relevant and not excessive
4. Accurate and where necessary, up to date
5. Not kept for longer than is necessary
6. Processed in line with the data subject's rights
7. Security
8. Personal information shall not be transferred to countries outside the EEA without adequate protection[180]

Taking into account the concepts of the Privacy Act 1974, the US DHS developed a set of Fair Information Practice Principles[181]:

1. Principle of Transparency
2. Principle of Individual Participation
3. Principle of Purpose Specification
4. Principle of Data Minimization
5. Principle of Use Limitation
6. Principle of Data Quality and Integrity
7. Principle of Security
8. Principle of Accountability and Auditing

Article 5 of Russian Law on Personal Data provides the following seven principles of personal data processing:

1. legality of goals, faithful and diligent conduct when processing personal data;
2. compliance with purposes determined and declared at the time of collection of personal data to process personal data exclusively within the scope of the authorities granted to them;

[179] Bygrave (2014).

[180] UK Information Commissioner's Office. Data protection principles. https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/.

[181] Department of Homeland Security. *Privacy Impact Assessment Update for TSA Advanced Imaging Technology*, 18 December 2015, p.3.

3. inadmissibility to integrate information databases created for different purposes;
4. inadmissibility to process personal data irrelevant to the purposes declared at the time of collection
5. compliance of scope and character of personal data to be processed and methods of processing with intended purposes of such data processing;
6. reliability of personal data, adequacy of personal data for processing purposes;
7. personal data shall be stored in a way that allows verification of the identity of the individual concerned only to the extent necessary for processing purposes. Personal data shall be destroyed upon achieving the set goals as well as when such goals cease to be relevant.

Other regulators, entities and researchers provide their own lists of principles. This fact does not allow making any exhaustive, generally accepted "official" list of all the principles and their names. On the one hand, the principles' components are quite similar. On the other hand, individual principles of data protection are not completely independent and there is great degree of overlap between them. In addition, they are not equal in the sense that they have different "weight". For instance, the purpose limitation principle is particularly important, since every aspect of processing – and any other principles – should be seen in the light of the purpose(s) of processing.

Thus, I have devised my own list based on the available materials:

1. Fair and lawful processing (discussed above within general principles)
2. Proportionality (discussed above)
3. Purpose limitation (a very broad and important principle)
4. Minimality (overlap with 3, but the emphasis is on ensuring limitation of personal data at the stage of data collection)
5. Non-retention of data beyond a certain period of time (overlap with 3 and 6, but in aviation security context is usually discussed separately, due to importance of limiting storage periods)
6. Data quality (common principle)
7. Data security (common principle)
8. Data subject influence (common principle)[182]

As for the issues of sensitivity and transborder transfer, due to some overlap, I will discuss them within principles 3 and 4. Thus, this research is supposed to cover all the important data protection principles that are usually indicated by different sources.

At the same time, in the aviation security field, exceptions and restrictions may apply to data protection principles. Similarly to possible limitation of the right to

[182] The principle of accountability is often argued to be a separate data privacy principle. Nevertheless, I consider it as an important emerging principle and will discuss it towards the end of this work in Chap. 8. The same applies to a more general transparency principle as indicated in Sect. 5.3.1.2 (broader than the one I discuss above within the principle of legality – legal transparency - and data subjects' right to be informed about data processing, see below).

privacy (see Chap. 2), the states – by way of a legislative measure – may be permitted not to apply data protection principles if such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard public security, public safety, prevention, investigation, detection and prosecution of criminal offences, protecting the data subject or the rights and freedoms of others, etc.[183]

Thus, data protection principles can be compromised, but essential conditions are that exceptions and restrictions must be provided by law, be necessary and proportionate – i.e. similar to requirements applicable to substantiate interference to the right to privacy. Thus, for the analysis and substantiation of privacy/data protection limitations, legal principles of privacy and data protection will be used in a complex all together. Concrete restrictions as well as issues of their substantiation will be considered in Chap. 7 with respect to concrete aviation security measures.

5.4.1 Purpose Limitation

As discussed in the Legality section, in relation to privacy, a connected term which is applied by the courts in the interference context is "legitimate aim". Due to its broadness, applying purpose limitation principles along with "legitimate aim" can be helpful to narrow the scope of legitimate purposes.

The purpose limitation principle is one of the fundamental principles of data protection, also known as "purpose specification" and "finality". Personal data must be collected for specified, explicit and legitimate purposes and not further processed in any way that is incompatible with those purposes (DPD Article 6(1)(b)). The notion "legitimate aim" was discussed above; "specified" and "explicit" purposes mean that the purposes cannot be unlimited and must be defined clearly and unambiguously, taking into account also the transparency and notification requirements, as well as prior checking mechanisms.[184]

The problem is that function creep – data collected for one purpose is used for another – is a particular concern for any smart technology, including those used in aviation security. In 2006, the presenters of IBM's "Smart Surveillance Solution" stated: "There is a lot of video captured and stored, and often the value of the video is unknown until well after the time of capture. Stored video is potentially valuable later".[185] This indicates very well how little awareness exists among technologists, security and business people about considering the possible negative effects.[186]

---

[183] See, e.g. § 6 of Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling adopted by the Committee of Ministers on 23 Nov 2010, GDPR Art.23 and Recital 73.

[184] Article 29 Data Protection Working Party (2004).

[185] Wright [et al.] *Sorting out smart surveillance*. In: Computer Law & Security Review. Vol. 26 (2010) p. 349.

[186] *Ibid.*

Consequently, aviation security, which extensively uses data initially collected for purposes other than security purposes – in particular, personal data deriving from the commercial sector – clearly contravenes the purpose limitation principle. However, the regulator may use different exceptions and derogations, primarily due to the security needs, to substantiate such use, e.g. by establishing international PNR agreements, see Special Part.

Yet, while the aviation security measures, as discussed, may easily fall within the "legitimate aim" criteria in relation to the data processing, the purpose limitation principle also implies some additional requirements, which can make the process of justification more complicated. As can be seen in the very term 'purpose limitation principle', the key word is limitation; accordingly, a number of other elements connected to purpose can be limited too.

For instance, the data should not be further processed for other purposes; purpose refers to *defined* purposes and not actual purposes, implying that the controller must have decided that personal data will be used for security purposes; how the data will be handled for security purposes if the data were initially collected for other, e.g. purely commercial purposes. In addition, with reference to both privacy and data protection, other criteria such as lawfulness and proportionality will serve as a limitation in order not to let the state go with new security measures as far as it wishes.

This principle generally implies that every aspect of how personal data are processed should be viewed in the light of purposes of the processing. This relates, for instance, to other data protection principles such as data quality and non-retention of data beyond a certain period of time discussed below.[187] Thus, clear aims and specific purposes may also contribute towards limiting the categories or types of data needed, the amount of people affected, the type of processing, the duration of storage, the quality of the data required, etc. This will mean better compliance with privacy and data protection rules. For aviation security, a logical idea could be that data collected pertaining to innocent people should not amount to data collected on targeted, suspected, or dangerous individuals. Biometric and sensitive data should be subject to additional rules: each part of the process from collecting, processing and storing such data must be taken into account to ensure that each element of the data processing is fully justified.[188]

An important criterion is compatibility. As Article 29 Working Party notes, further processing for a different purpose does not necessarily mean that it is automatically incompatible; this needs to be assessed on a case-by-case basis.[189] Working Party distinguishes formal or substantive assessment. The former compares the purposes that were initially provided by the data controller with any further uses to find out whether these uses were covered. Substantive assessment is more flexible, pragmatic and effective, since it takes into account the way the purposes are (or should

[187] See, e.g. Norwegian Personal Data Act of 2000, §11.

[188] Article 29 Data Protection Working Party (2014a).

[189] Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation, Brussels, 2 April 2013 (2013a), p. 21.

be) understood, depending on the context.[190] In order to assess compatibility, the following factors can be helpful:

- the relationship between the purposes for which the data have been collected and the purposes of further processing
- the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use
- the nature of the data and the impact of the further processing on the data subjects
- the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects[191]

This principle also implies that personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law (DPD Article 6). Of course, disclosure can be of different types, e.g. domestic sharing and across borders. With regard to domestic sharing, limitation concerns first persons within the organization and secondly sharing with other organs. Both, in principle, should not involve persons or entities that are unrelated to the aviation security activities. Ideally, the persons who have access to personal data should be restricted to minimum and, should there be a disclosure of personal data by such officials, the applicable punishments should be established.[192]

This is especially relevant for situations when not all personal data to which aviation security organs needs access are processed by them, and they may need access to data originally collected by other organizations for other purposes, such as PNR collected by airlines. To safeguard the data, access to the system and the number of people who have access to data should be limited, as well as the length of time that the data is stored, and compliance with other data protection principles should be ensured. For example, the ICAO PNR Guidelines require that the state should ensure that every state authority having access to personal data ensures the appropriate level of data protection.[193]

It can be seen that this principle overlaps with and may contribute to compliance with other principles, both general and data protection principles. This makes it one of the most important for the researched area, with the circulation of personal data not only among multiple entities, but transborder as well.

[190] Article 29 Data Protection Working Party (2013a), p. 21.

[191] For more detail, see Article 29 Data Protection Working Party (2013a), pp. 23–27.

[192] Aquilina (2010) p. 142.

[193] §2.12.

5.4.2 *Minimality*

As discussed in Chap. 2, the biggest challenges to data protection today are technological developments, globalization and Big Data. In aviation security, state organs, airlines, airports and other entities, via different technologies, are capable of collecting huge amounts of different types of personal data from multiple sources (see Chap. 6), which are then processed for security purposes and other uses.

These huge opportunities create advantages for aviation security, but challenges for data protection. The minimality principle – also known as "data minimization" – can contribute towards limiting data collection. It is stipulated in DPD and Convention 108 (Article 5(c)), which both are aimed at ensuring minimality at the stage of collection: personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed (DPD Article 6(1)(c)). It requires that the minimum amount of personal data to be collected and processed, limiting this amount to what is absolutely necessary to achieve the purpose for its collection and processing.[194]

In simple words, keeping in mind the purposes of processing, the data controller should identify the minimum amount of personal data needed to properly fulfil these purposes. Accordingly, data can be collected only in that necessary minimum amount – not more.[195]

This principle is aimed at preventing or reducing, to the greatest possible degree, the processing of personal data: in fact, many purposes can be actually achieved without recourse to personal data, or by using really anonymous data, even though they may initially seem to require the use of personal information.[196]

It can be seen that this principle is dependent on the purpose limitation principle. It is also very close to the proportionality principles, since for determination of how much data is needed, various interests – data protection interests and other interests – should be considered. It also relates to the next principle below – non-retention of data beyond a certain period of time – which is also aimed at minimization, but minimization of aspects such as data storage.

Moreover, minimality contributes to data security too: the rule that the minimum amount of data should be kept for the minimum amount of time is supposed to reduce the likelihood of data being leaked, lost or misused.[197]

For instance, a good practical illustration can be found in the employment field, where the employer's access to a part of employee's personal data (namely, speed, fuel consumption and travel times) can be limited via programming. This is supposed to protect the employee's personal data, which will not be open to the

[194] Bygrave (2014) pp. 151–152.

[195] UK Information Commissioner's Office. Data protection principles. https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

[196] Article 29 Data Protection Working Party (2004).

[197] Gilbert. *Dilemmas of privacy and surveillance: chaljenges of technological change* (2007) p. 26.

employer, but can still exist in the system and be useful for the employee to evaluate his driving habits.[198] Similarly, some information about air passengers, although kept in airlines' systems, could be secured by limiting authorization for access only to passengers, thus, contributing to the minimality principle and other principles.

A problem which arises is how to classify all the potentially collected data: which are needed and which are excessive. Apparently, with current risk-based and intelligence-led aviation security (see Chap. 6), security organs may consider that any pieces of information may be useful for predicting threats, thus, may be unwilling to limit them at the stage of collection.

A special treatment in the terms of minimality deserves sensitive data (see Chap. 2), which collection at the initial stage must be justified by stricter requirements. In order to assess the sensitivity of data, the context of the processing should be taken into account.[199] But in every respective case, such practices should be checked to ensure that they satisfy legal requirements. In addition to the applicability of the exemptions, other principles should be applied as well: e.g. whether the collection and usage of this data is justified and really needed, or whether collection is unnecessary and excessive.

5.4.3 Non-retention of Data Beyond a Certain Period of Time

According to DPD Article 6(1)(e), personal data can be kept for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. This constitutes the principle of non-retention of data beyond a certain period of time (for convenience, "data retention principle"): data should be stored only for such periods as stipulated by law and should be deleted after the data is no longer relevant.

This principle is closely related to the principles of proportionality, minimality, purpose limitation and data quality. First, data should not be kept unnecessarily; these data must be deleted as soon as they are no longer necessary for the specific purpose.[200] Secondly, deletion of personal data when no longer needed is supposed to reduce the risk of the data becoming inaccurate, outdated or irrelevant.[201] Moreover, similar to the data minimality principle, keeping data for the minimum amount of time is supposed to enhance data security, reducing chances of data misuse.

The data retention period is commonly an essential item in the analysis of a concrete aviation security practice or regime, e.g. storage of PNR data, storage of

[198] Schartum. *Rettslige aspekter ved feltteknologi i arbeidslivet* (2013) p. 73.

[199] Article 29 Data Protection Working Party *Opinion 3/2012 on developments in biometric technologies* (2012b).

[200] European Committee on Legal Co-operation (2003).

[201] UK Information Commissioner's Office. Data protection principles. https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

CCTV images, etc. In particular, the data retention issues cause concerns if personal data on all passengers – including innocent people – are stored rather than only on suspects, targeted individuals and the like.

Case law around ECHR also clearly confirms that storage of personal data for longer than is necessary contradicts the "necessary in a democratic society" test.[202] Thus, excessive data retention also means interference with privacy.[203] Typically, a concrete practice often violates all the related privacy and data protection principles (see above). As the Article 29 Working Party notes, failure to specify the purpose, in terms of data protection, may lead to a breach of the minimality and data retention principles; in terms of privacy, this will mean that the legitimate aim criterion suffers, leading in turn to proportionality concerns.[204] For instance, the lack of defined purposes, disproportionality and lack of a clear link with the purpose for personal data retention are applicable pursuant to Article 29 Working Party, to PNR.[205]

Accordingly, it is essential to stipulate rules on data retention and re-evaluate such retention periodically to ensure compliance with a person's right to a private life and valid data protection law,[206] making this principle important per se and also an important condition for ensuring other principles discussed in this chapter.

5.4.4 Data Quality

The data quality principle requires that personal data must be relevant, accurate, timely, complete, kept up to date (DPD Article 6(1)(c,d)). Multiple terms are used, and in different legal instruments, there can be variation in terminology, scope and stringency of monitoring requirements.[207] But in general, two aspects of data quality can be noted: the first concerns validity – data should be valid with respect to what it describes, and secondly, data should be relevant and complete regarding the purposes of processing.[208]

The data quality principle is dependent on the principle of purpose limitation and is close to the minimality principle requiring that personal data should be adequate. Ensuring the accuracy of personal data is supposed to contribute to data minimality.

Ideally, according to this principle, persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission as well as to

[202] See *S and Marper v. the United Kingdom,* No. 30562/04 and 30566/04, 4 Dec 2008.

[203] Article 29 Data Protection Working Party (2014a).

[204] *Ibid.*

[205] *Ibid.*

[206] *Ibid.*

[207] See further Bygrave (2014) pp. 163–164.

[208] Bygrave (2014) p. 163.

ensure that they are regularly updated or kept current when the information contained in a file is used and for as long as it is being processed.[209]

However, in practice, persons in some cases have to contact the data collectors to rectify/delete various inaccuracies in their data. This can be done via realizing another data protection principle – data subjects' influence. This will be discussed below, but in general, it may be difficult for a person to rectify/delete inaccuracies. Thus, the realization of the principle of data quality is dependent on the provision of particular measures to be undertaken by the data controller to ensure that data is valid, accurate, relevant, etc.

5.4.5 Data Security

Personal data should be processed in a secure mode and protected by security safeguards against such risks as accidental or unlawful destruction, loss, alteration, disclosure, access, as well as any other unlawful forms of processing.[210] This is principle of data security. Clearly, there is no "one size fits all" solution to data security universal for all spheres and all contexts, thus, appropriate security measures should be adopted on a case-to-case basis.[211]

As discussed in Sect. 2.2.2.3, a part of aviation security is information security which is aimed to protect the respective systems against attacks. The latter can have very serious dramatic consequences. This substantiates enhanced requirements to information security. Consequently, since undertakings on data security of personal data often come parallel with broader undertakings on information security, the requirements may be enhanced too.

It should be also noted that in the considered jurisdictions, the application of this principle – or the approach to security requirements – differs greatly between Russia and the EU/USA.

In the EU/USA, the laws generally indicate that the methods of data protection must be reasonable and sufficient, leaving the implementation of these principles to the controller, who will take full responsibility if the measures taken are insufficient. Thus, general technical standards are not provided. For example, Article 17(1) of DPD provides that data controllers and processors must implement two types of appropriate security measures: technical and organizational; Recital 46 stipulates that these types of measures should be taken both at the time of the design of the processing system and at the time of the processing itself. In the EU, there is a considerable disparity in the security requirements of Member States: while some

[209] The United Nations General Assembly Guidelines for the Regulation of Computerized Personal Data Files.

[210] Art. 17(1) of DPD, Art. 11 of OECD Privacy Framework 2013.

[211] UK Information Commissioner's Office. Data protection principles. https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

specify more details, in the UK, for example, the requirements simply repeat those of the DPD.[212]

Data security requirements in Russia are very comprehensive and detailed. It is even argued that this law is aimed largely at stipulating technical requirements to personal data processing – so complicated that they are analogous to protection of state secrets – rather than protection of data subjects.[213]

Data controllers must provide technical measures according to the security levels determined by the RF Government.[214] The choice of the means of protection of personal data made by the controller in accordance with the regulations adopted by the FSB and the Federal Service for Technical and Export Control of the RF (FSTEC). In practice, concrete methods and techniques appear to be excessive and expensive: expenses for security equipment (which must be produced by companies licensed by the FSTEC and the FSB) constitute up to 200% of the annual turnover and then 10–15% of the cost for annual maintenance.[215] But in reality, personal data in Russia are usually stolen through bribery of responsible employees rather than by breaking the security systems, so all these requirements may be devoid of meaning and effectiveness.

Nevertheless, the aim of all the regimes is uniform – to keep personal data secure. Particular aviation security technologies dealing with personal data imply concrete security undertakings and are very similar across jurisdictions, as will be discussed in Special Part.

5.4.6 Data Subject Influence

It is not only the controller who ensures that the data are kept secure, accurate and so on. The data subjects also have their self-interest at stake and thus should have the right to participate. This is another fundamental principle of data protection – data subject influence (sometimes also called a principle of cooperation).

This principle refers to a number of rules providing various rights of individuals. According to Bygrave, the relevant rules include (i) the rules to make people aware of data-processing activities in general, (ii) to be aware of basic details of the processing of data on themselves (including the rules on collecting data directly from data subjects, rules to orient data subjects directly about certain information on processing, and rules prohibiting processing without the consent of data subject), (iii) the right to gain access to data kept on them, and (iv) to object to others' processing of data on themselves (which is close to the rules prohibiting some types of

[212] Esayas (2015) p. 16.

[213] Chernova (2013).

[214] Resolution of Government of 1 November 2012 N 1119 On approval of requirements for the protection of personal data during their processing in information systems of personal data.

[215] Modern Telecommunications Russia. *The Council of Federation adopted Personal Data Law*, 21 July 2011. http://www.telecomru.ru/article/?id=6067

processing without data subject's consent) and to demand that the data be rectified or erased.[216]

The UK ICO provides the following list of relevant rights:

1. a right of access to a copy of the information comprised in their personal data;
2. a right to object to processing that is likely to cause or is causing damage or distress;
3. a right to prevent processing for direct marketing;
4. a right to object to decisions being taken by automated means;
5. a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
6. a right to claim compensation for damages caused.[217]

As can be seen, the principle of data subject influence relates to a wide category of rules, but they overlap greatly. Below, this principle will be discussed taking into account the rules indicated by Bygrave.

The DPD contains duties of information and orientation of the data subject: first, general information should be provided to public, and it should be easily accessible and easy to understand. This relates to the more general principle discussed above within the legality principle, specifically, the principle of *publicatio legis*/transparency. As noted, security needs may limit access to legal information if the latter falls within a restricted category.

Data subjects should be informed of the data processed on them, purposes of such processing and the identity of who is collecting their data. Information should be also given about the measures for protection of the data, whether there is any data share, the identity of the officer collecting and responsible for the data, procedures available for redress and contact information for persons to whom to address questions or concerns about data retention (Articles 10–11).

In general, the data subject can object at any time to the processing of data relating to him on compelling legitimate grounds relating to his particular situation.[218] In addition, the ability to object is connected to the rules prohibiting certain data processing without the data subject's consent[219] (DPD Articles 7–8). The latter means "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (DPD Article 2(h)). It should be given unambiguously (DPD Articles 7(a)) and explicitly ((DPD Articles 8(2)). The "unambiguous" means that, as a general rule, data subjects should give consent to the terms and conditions of the processing of his/her personal data, and their actions should leave no doubt that they have given

[216] Further see Bygrave (2014) pp. 158–163.

[217] UK Information Commissioner's Office. Data protection principles. https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

[218] Article 29 Data Protection Working Party (2004).

[219] Bygrave (2014) p. 160.

consent.[220] "Explicit" consent is a more stringent requirement – there must be specific request for permission from the data subject followed by specific reply.[221]

The problems which arise concern ensuring the criteria informed, specific (or explicit) and freely given consent. In principal, free consent is difficult to realize in reality: in data processing, data subjects are almost always the weakest party, making consent a formality.[222] The point is that aviation security procedures fundamentally differ from free choice. Passengers and the security organs are not equal in powers, and passengers cannot object to screening or personal data collection unless they accept not to fly at all.

Moreover, the exceptions from the duty to obtain consent are quite widespread and include such categories as processing being necessary for the performance of a contract or for the performance of a task carried out in the public interest, in order to protect the vital interests of the data subject, etc. (DPD Article 7). Clearly, the interests of aviation security may fall under any of the exceptions and thereby justify most instances of processing.

As a result, genuine, freely given and informed consent in aviation security can hardly be ensured or required either, and in practice, people are not able to consent or reject airport surveillance.[223]

Further, data subjects should be allowed to access their data and make corrections to any inaccurate data (DPD Article 12, Article 8 of the CFREU). This allows a data subject to have an indirect right of access to carry out checks over public security files to ensure that the file contents are accurate. It is common that stipulating the rights of data subjects by national data protection law are supported by corresponding provisions on data controller's obligations to provide these rights to data subjects.

For instance, the Russian Personal Data Law stipulates the rights of the data subject to obtain information related to the processing of his/her personal data, to access it, to redress breaches of personal data processing, to correct, block or destroy personal data (Article 14) as well as respective duty of data controller to provide these opportunities to data subject (Articles 20 and 21).

It is also essential that the agencies concerned – i.e. data controllers – must have guidelines or procedures on access to and sharing of personal data in order to ensure this obligation to provide ensure the data subjects' rights to access, rectification and deletion.[224] However, in practice, there appear difficulties with the duties of access/rectification: it is very often that data controllers have no established procedures and mechanisms thus are not capable to provide these rights. Notable examples are unsuccessful attempts to get air passenger personal records from authorities and airlines, which will be discussed in Special Part.

---

[220] *Ibid.*

[221] *Ibid.*

[222] Gutwirth et al. (2011) p. 27.

[223] Gilbert (2007) p. 33.

[224] Aquilina (2010) p. 142.

5.5 Concluding Remarks to Chap. 5 and to General Part

The principles, as discussed, are the key elements of this research. They express the essence of the considered values – aviation security and privacy/data protection – and constitute the basis of the applicable regulation, allowing us to identify the privacy/data protection concerns that arise from concrete aviation security measures and how they can be dealt with.

The key principle is the proportionality principle. It has two roles: first, it is valuable as such, as one of general legal principles of which the core essence is the comparison of different values. Thus, it can be used as an instrument for finding proportionality between a number of values: threats and risks, costs and benefits, the need to interference and the need to protect a human right, ultimately – between aviation security and privacy/data protection.

Secondly, it is valuable since it unites different factors and issues discussed in General Part of this research into one "puzzle" allowing analysing aviation security versus privacy dilemma from multiple corners.

In particular, aviation security issues discussed in Chap. 4 have impact and/or define aviation security. Similarly, privacy/data protection concepts, regulation (Chap. 2) and principles (Chap. 5) define privacy/data protection. At the same time, as discussed above, security decisions and principles of aviation security discussed in Chap. 4, privacy and data protection principles discussed in Chap. 5, as well as all other relevant human rights discussed in Chap. 3 have impact on the proportionality of the aviation security regimes.

It can be seen that some factors perform a double task. For instance, with reference to the section on aviation security, the rationale of aviation security decisions and aviation security principles explains, on the one hand, the logic of regulators adopting and using different aviation security techniques and methods. On the other hand, the security regulators use the proportionality principles to find a balance between threats and risks, costs and benefits. Cost and benefits may include costs in the form of privacy risks and benefits, if a measure contributes to passenger experience, for instance, respects or even enhances privacy. These issues, as well as issues of effectiveness of aviation security measures, overlap with the use of proportionality principle from privacy/data protection perspective.

Altogether, these factors permit the establishment of the approach to the aviation security and privacy dilemma that will be used in the Special Part to evaluate the impact on privacy/data protection and the proportionality of the selected aviation security measures. Other relevant human rights will be evaluated additionally to better assess proportionality of the regimes.

Accordingly, the impact of aviation security measures on passenger rights will be assessed using the following scheme. First, the applicability of privacy/data protection to the selected aviation security measures should be analysed using their technological and operational characteristics and knowledge from Chaps. 2 and 3.

If positive, it should be established whether there are relevant limitations, concerns or problems. If positive, the next step is to consider whether the limitations,

concerns or problems can be justified. For these two steps, legal principles of privacy/data protection indicated in Chap. 5 will be used, taking into account knowledge from Chap. 4 and other chapters. Other human rights discussed in Chap. 3 will be evaluated similarly, but on a limited basis, in the amount necessary to indicate additional problems, if any.

Clearly, proportionality is not a fixed condition and can range from "proportionate" in the best case to "non-proportionate" in the worse. The first condition is perfect, implying that there are either no concerns, or the concerns are outweighed by the security needs. Apparently, practical results from evaluation of particular measures will differ, entailing that each must be placed somewhere between the poles. At the same time, however, it will be possible to evaluate an aggregated effect of all the considered measures on all privacy and data protection principles as well as on all human rights. Consequently, it will allow – with certain limitations – evaluation of contemporary aviation security regimes as such.