TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Essi Lumiaho

THE IMPLICATIONS OF ADVANCEMENTS IN SMART BORDERS PACKAGE BIOMETRIC DATA COLLECTION AND STORAGE TECHNOLOGY ON THE RIGHTS OF THE INDIVIDUAL IN THE CONTEXT OF THE EU CHARTER OF FUNDAMENTAL RIGHTS

Bachelor's thesis
Programme HAJB08/17 Law, specialisation European Union and International law

Supervisor: Jenna Uusitalo, M.A.

Tallinn 2020

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 12,032 words from the introduction to the end of conclusion.

Essi Lumiaho ……
(signature, date)
Student code: 177706HAJB
Student e-mail address: essi.lumiaho@gmail.com

Supervisor: Jenna Uusitalo, M.A.:
The paper conforms to requirements in force

……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence

……
(name, signature, date)

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
ECJ	European Court of Justice
EES	Entry-Exit System
EU	European Union
EUCFR	European Union Charter of Fundamental Rights
EURODAC	European Asylum Dactyloscopy Database
EUROPOL	European Union Agency for Law Enforcement Cooperation
eu-LISA	European Union Agency for the Operational Management of Large-Scale IT Systems
GDPR	General Data Protection Regulation
JHA	Justice and Home Affairs
MS	Member State
NUI	National Uniform Interface
PNR	Passenger Name Record
RTP	Registered Travellers Programme
SIS	Schengen Information System
TCN	Third-country nationals
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
VIS	Visa Information System

ABSTRACT

Freedom of movement and the right to data protection are core fundamental rights upon which the European Union is built. However, in light of recent terrorist atrocities, these rights have been called into question, with lawmakers tightening the border surveillance and introducing new IT systems. Systems, such as the Entry-Exit System, as part of the Smart Borders Package, have been enforced to protect the Union by collecting biometric data and tracking alien movement in the Schengen area. The question is raised as to how the EU manages to abide by the fundamental rights law, while maintaining protection at its borders through continuing advancements in data processing.

The issue with the novel implementation of border management, is that it has implications on, and may contravene current legislation laid down in the EU Charter of Fundamental Rights. The aim of this thesis, therefore, is to evaluate the extent of infringement upon the right to data protection by fingerprint collection in the EES. This aim is investigated through a comprehensive and qualitative research methodology.

By applying the principle of proportionality to the conflict of rights, this thesis finds a significant limitation on the rights of the data subjects, but the measure is not imposing a direct impact on the fundamental right to data protection. Furthermore, this thesis contributes to the continuous development of discourse centred on consistency when implementing the EU law.

Keywords: European Union, Entry-Exit System, Biometric Data, EU Charter of Fundamental Rights, Data Protection

INTRODUCTION

As a result of the Fourth Industrial Revolution, new technological advances have emerged and brought a change in how societies interact[1]. In a rapidly evolving digital world, data protection is one of the most recognisable areas of recent investment by the European Union (EU). The digital evolution has brought about a paradigm shift in the way personal data processing is a necessity for a modern and connected way of living. Individuals, communities and societies now exist in this new world, where the identification of a person has become of great importance in relation to all human action, whether active or not. As with any change, the law needs to keep up and ensure concrete protection for the data subjects. These technological advancements, and the pace of change needed to keep up, present the problem of implications and the contravention of legislation on the fundamental rights.

The aim of this bachelor thesis is to provide assessment on and evaluate to what extent the capture and storage of biometric data from visa-exempt third-country nationals (TCN) traveling to and from the Schengen area may infringe the rights of the individual. This statement will be framed in the form of the hypothesis that: The capture and storage of biometric data from visa-exempt TCNs, as set out in the Entry Exit System (EES), is in conflict with the principles of fair processing and proportionality.

With the purpose of investigating the hypothesis, this thesis will seek to answer the following research questions: Firstly, whether the capture and storage of biometric data from visa-exempt TCNs as set out in the Article 17 1. (c) of the EES Regulation 2017/2226 contravenes Article 8.2 of the European Union Charter of Fundamental Rights and secondly, how the Regulation can comply with Article 8.3 of the EU Charter. Furthermore, this thesis will discuss the measures in place to ensure that the EES Regulation conforms to the principle of proportionality provided in the EU Charter of Fundamental Rights.

[1] Schwab, K. (2017). *The Fourth Industrial Revolution*. Redfern: Currency Press. p 7.

The proposed research within this thesis will allow for a thorough investigation into the relationship between the EES, The EU Charter on Fundamental Rights, General Data Protection Regulation (GDPR) and the legality surrounding the freedom of movement within the Schengen area and the EU. With this proposition in mind, the author of this thesis regards the research problem as a theoretical contradiction and thus presents the following research problem; Advancement in data collection and storage technology will have implications on and therefore, may contravene current legislation laid down in the EU Charter on the Fundamental Rights of the Individual.

In order to prove or disprove the hypothesis, the author of this thesis proposes to employ an entirely qualitative methodology. This thesis will utilise measures such as doctrinal research, legal interpretation and analysis of legislation. Academic sources, books, journals and existing cases are used to support assertions presented in this thesis. These references have been chosen from a wide variety of origins and give the author of this thesis as full of a view of the legal framework as possible. Furthermore, the references will be used to formulate the author's own conclusions to the proposed hypothesis and to answer the research questions.

This topic is of importance because, one of the key fundamentals of the EU Charter is the freedom of movement within the Schengen area. It is also acknowledged that it remains the duty of the Member States to provide protection for all persons in Europe, however, there is a need for discussion on whether the new practices of collecting and storing biometric data infringe rights of the individuals, to the point it contradicts the EU's own Charter. As a discipline, the gathering and storage of fingerprints as biometric data is relatively new for visa-exempt nationals and therefore, a question on the legitimacy of the regulation arose. As such, it is the author's opinion that discussion should be maintained on the fundamental rights of the individual with respect to the current form of the EU Charter in relation to the processing of biometric data.

1. ENTRY-EXIT SYSTEM AND THE SMART BORDERS PACKAGE

1.1. Background

In 2008, the European Commission began to work on a set of legislative proposals to modernise the European border management system[2] through co-operative tools for Member States (MS), with a view to meet its objectives of enhancing security and facilitating travel for third-country nationals[3]. At the time of the publication of the *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, visa-exempt third-country nationals were only obliged to undergo border controls upon arrival at the physical border, but not at any point prior[4].

The Entry-Exit System was one of the three legislative proposals forming the Smart Borders Package initiative, together with proposals for a Registered Travellers Programme (RTP), facilitating the pre-vetted *bona fide* travellers and a proposal on amendment to the Schengen Borders Code[5], introduced by the European Commissioner for Home Affairs in February 2013[6]. The Smart Borders Package was established to facilitate an open and secure Europe that would accelerate the border controls in each Member State[7]. However, in light of privacy issues, the Smart Borders Package was pulled back, and the Commission endeavoured to ensuring the requisite changes to the EES were made in the first months of 2016[8]. Nonetheless, the idea of a

[2] European Union, European Commission. (2008). *Commission Staff Working Document: Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Report on the evaluation and future development of the FRONTEX Agency: Impact assessment*, 5.3. policy option 3.
[3] European Union, European Commission. (2008). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Preparing the Next Steps in Border Management in the European Union*, p 4.
[4] *Ibid.*
[5] Bourbeau, E. (2017). *Handbook on Migration and Security*. Cheltenham, United Kingdom: Edward Elgar Publishing, p 241.
[6] Sontowski, S. (2018). Speed, Timing and Duration: Contested Temporalities, Techno-political Controversies and the Emergence of the EU's Smart Border, *Journal of Ethic and Migration Studies*, 44 (16), p 2733.
[7] Bourbeau, *supra nota* 5.
[8] European Union, European Commission. (2016). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399*, p 6.

centralised identification system based on biometrics has remained legitimate throughout the process.

In light of concerns surrounding the Smart Borders Package, The Commission withdrew the initiative and abandoned its proposal for a regulation on an RTP. In turn, the proposals for the establishment of an EES and the amendment of the Schengen Borders Code were revised. The amendment of the Schengen Borders Code integrated the technical changes in the new EES proposal.[9]

The Commission reasoned the need to establish an EU EES in its 2016 proposal through three arguments as to the issues of border check delays and quality of service for third country nationals, lack of systematic and reliable identification of persons exceeding their allowed stay, and contingency of internal security with respect to terrorism and serious crime. The Commission argued, that the replacement of the slow and unreliable system of passport stamping would not only allow for a more effective monitoring of authorised stay and border checks, but also to hand explicit data to border guards on refusals of entry. The EES was declared as a preventive solution to the concern of irregular immigrants and persons exceeding their authorised stay, as it would support controls on "overstayers" with precise information and storage of biometrics of all visa-exempt persons and subsequently, compare them to the database of Visa Information System (VIS).[10]

The call to establish a new database to safeguard the Union security only intensified in the wake of terrorist attacks in France in 2015. A large proportion of the MS were supportive of the construction of a database on monitoring third-country nationals traveling to and within the Union for purposes preventing the actions of terrorists[11], as it was a belief amongst the advocates for the system, that such a database would make, facilitate and accelerate the process of law enforcement agencies catching criminals[12]. Moreover, national border, visa and immigration authorities and

[9] European Commission. (2016). *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES),* p 2.
[10] *Ibid.*
[11] Bourbeau, *supra nota* 5, pp 241-242.
[12] Lwin, M. (2010) Privacy issues with DNA databases and retention of individuals' DNA information by law enforcement agencies: the holding of the European Court of Human Rights case S and Marper v. United Kingdom should be adapted to American Fourth Amendment jurisprudence. *Information & Communications Technology Law*. 19 (2), p 193.

European Union Agency for Law Enforcement Cooperation (EUROPOL) were provided access to EES data[13].

1.2. Overview of the Entry-Exit System

The Entry-Exit System is an extensive IT system which monitors third country nationals who cross the borders of the European Union. The system serves as a tool for not only improving the management of Union borders, but also for the prevention of irregular migration, through the method of monitoring overstayers, and combatting crime and terrorism.

As a Schengen instrument, the data from third country nationals is documented into the Entry-Exit System in the Schengen Member States. Operational management and development of the EES is the responsibility of The European Union Agency for the Operational Management of Large-Scale IT Systems (eu-LISA). The EES is composed of a Central System, which, through a connection to a National Uniform Interface (NUI) in each MS, the authorities are able to access the national border infrastructures.

Identities of third-country nationals are recorded to the system with alphanumeric data, four fingerprints, facial recognition and non-biometric data from their travel documents. This personal data is connected to the passengers' respective record of entries and exits, and travel documents are no longer stamped, as the practice has been abolished as of January 2020. Considering the Regulation 2017/2226, information on dates and places of entries and exits of third-country nationals admitted for a short stay are recorded into the EES[14], irrespective of requirements for a Schengen visa or those who have been refused entry[15], and the system automatically establishes the maximum 90 days length, in any 180-day period, of allowed stay under the provisions provided by the Schengen Borders Code[16].

[13] Bourbeau, *supra nota* 11.
[14] Bossong, R., Carrapico, H. (2016). *EU Borders and Shifting Internal Security: Technology, Externalization and Accountability.* Cham: Springer. p 28.
[15] OJ L 327, 9.12.2017, recital 9.
[16] Bourbeau, *supra nota* 5, p 242.

1.3. Processing of personal data and Article 17 1. (c)

The collection of fingerprints has served as a long-standing method in crime prevention and as a tool utilised in criminal investigations. Fingerprints are distinctive to a person and their individual ridges and curves are permanent traits[17], allowing for personal identification data. Any damage on the surface of the skin may temporarily alter the appearance of a fingerprint, however, once the finger is healed, the original curves to one's fingerprint will re-emerge[18]. Fingerprinting maps the individual ridges and their curves on the surface of the finger, and with such unique information, fingerprints are considered one of the most reliable ways of identifying people[19]. Nonetheless, due to the distinctive nature of fingerprint data, it is of significant value to invest in its protection as possible harmful exploitation methods are yet to be fully understood[20].

The GDPR states that biometric data shall not, as a general rule, be processed for the sole purpose of uniquely identifying a natural person unless Union or MS law provides the contrary.[21] For the purpose of this thesis, it is of great importance to acknowledge the contextual relationship between the EU legislation on data protection and biometric data processing activities, in order to further understand how the EES may impose restrictions on the fundamental rights of individuals in the EU area.

Estimates, prior to the 2020 COVID-19 outbreak, suggested that the EES will produce a register containing 167 million records in its first year of operation[22] and 269 million records within five years[23]. The processing of large groups of data subjects in EU Justice and Home Affairs (JHA) databases face the risk of encountering significant social harm, as the Entry-Exit System recording fingerprint data, *inter alia,* uses parameters with an automated decision-making ability, in which the data subjects are profiled[24]. Despite the objective of battling actions in violation of Community law, the selection of persons deemed as potentially hazardous in the EES allows for a possibility

[17] Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S. (2009). *Handbook of Fingerprint Recognition*. (2nd ed.) London, England: Springer, p 10.
[18] Lwin, *supra nota 12,* p 32.
[19] Maltoni, Maio, Jain, Prabhakar, *supra nota*, p 12.
[20] Nguyen, F. G. (2018) The Standard for Biometric Data Protection, *Journal of Law & Cyber Warfare*, 7(1), p 63.
[21] OJ L 119, 27.4.2016, Article 9.
[22] Jeandesboz, J. (2016). Smartening Border Security in the European Union: An associational inquiry. *Security Dialogue,* 47 (4), p 298.
[23] Jeandesboz, J. (2017). How to make sense of information and data processing. In: A. R. Servent, F. Trauner (Eds.), *Routledge International Handbooks.* New York, USA: Routledge, part III, section 15.
[24] Bigo, D., Carrera, S., Hayes, B., Hernanz, N., Jeandesboz, J. (2012). *Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An evaluation of Current and Forthcoming Proposals,* p 10.

to conduct biased ethnic profiling[25]. National and EU law enforcement bodies are presented with the challenge therefore, of how to identify the potentially dangerous persons whilst refraining from discrimination on the basis of nationality or ethnicity[26].

The EES is designed to interoperate with the Schengen Information System (SIS) and the VIS, and the information available in SIS, for easing the process of detaining criminals. Prior to the establishment of the EES, there was no possibility of recording exits of persons, regardless of any possible benefit from the EU visa waiver. As an example, the VIS collects fingerprint data from visa applicants before they step onto the European soil[27], whereas the EES focuses on the opposite, it gathers fingerprints and data starting from the border entry, during the stay and until the exit. With the addition of the EES, and the possibility to compare biometric data among these three systems, the direct communication channel has presented the MS' border authorities with the ability to monitor illegal migration of non-visa nationals.

Article 17 of the Regulation 2017/2226 establishes the categories of personal data of visa-exempt TCNs, which will be entered into their individual files. The third paragraph defines fingerprint data as, biometric data sourced from the right hand excluding the thumb, and if this data is unobtainable from the right hand, the fingerprints will be collected from the left hand[28]. All entry and exit data of TCNs are logged into their individual files. An individual file is retained in the EES for at least three years and a day. If the TCN makes multiple entries and exits within the retention period, the length of time the record is kept for is extended by an additional three years and one day. The extension period will repeat for every entry and exit made. Conversely, once a TCN leaves the Schengen area, the record of that specific entry and exit will be removed after 3 years[29].

1.4. Legitimate objectives and justifications

The most important principle limiting the EU's competence is the principle of conferral, according to which, the Union is mandated to perform within the boundaries of its competencies bestowed

[25] Schermer, B. W. (2011) The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*. 27 (1), p 47.
[26] Bigo, Carrera, Hayes, Hernanz, Jeandesboz, *supra nota* 24, p 39.
[27] *Ibid.*, p 6.
[28] OJ L 327, 9.12.2017, recital 16.
[29] *Ibid.*, Article 34.

by the MS in order to meet its objectives. The extent to which the Union may exercise its competence is identified in the Treaty on European Union (TEU), also known as the Maastricht Treaty, as subject to principles of subsidiarity and proportionality.[30]

The principle of subsidiarity, introduced by the TEU, allows the Union to undertake actions in sectors where the competencies do not always lie solely with the Union, but are shared with the MSs[31]. According to Article 5(4) TEU, any actions taken by the Union, in compliance with the principle of proportionality, shall not exceed what is essential for the attainment of the objectives of the Treaties.[32]

In Article 77, the Treaty on the Functioning of the European Union (TFEU), commonly referred to as the Treaty of Lisbon, establishes legitimate objectives upon which the Union may base any policies, with reference to border checks, asylum and immigration. Persons crossing the external border, in accordance with the Union's framework, must be subjected to border checks. One of the cornerstones of the asylum and immigration policy is the effective monitoring of cross-border movement, because the lack of a common policy results in a lower threshold for border checks, as well as soaring costs and disintegration of trust between the MSs[33].

In the *S. and Marper* landmark case, considering the storage of sensitive biometric data, the European Court of Human Rights (ECtHR) ruled that fingerprints are "capable of affecting the private life of an individual" as they contain unique information about the individual concerned[34]. Furthermore, the ECtHR noted that the underlying issue within the relationship of law in the biometrics and privacy is, that the technological advancements are progressing at a much faster pace than the law is able to foresee[35]. The decision of ECtHR gives reason to question the ability of data processing technologies to respect the right to protection of such sensitive categories of data, and ultimately, the fundamental rights in Europe.

[30] OJ C 326, 26.10.2012, Article 5.
[31] De Búrca, G. (1998) Principle of Subsidiarity and the Court of Justice as an Institutional Actor. *Journal of Common Market Studies*, 36 (2), p 218.
[32] European Union, European Commission. (2013). *Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP)*, p 3.
[33] De Capitani, E. (2014). The Schengen system after Lisbon: from cooperation to integration. *ERA Forum,* 15, p 113.
[34] S. and Marper v. United Kingdom, no. 30562/04 and 30566/04, point 84, ECHR 2008.
[35] Lwin, *supra nota* 12, p 199.

This case is relevant for consideration, albeit not directly from an EU institution but from the European Court of Human Rights, due to the fact that the European Convention on Human Rights (ECHR) serves as the ancestor to the Charter, with the basis for right to privacy. The rulings of the ECtHR do not hold binding force over the EU bodies per se, but still remain a highly influential adjudicator with reference to any action, because, the EU has agreed to take into account the fundamental freedoms guaranteed by the ECHR across all fields of operation[36]. For the purposes of this thesis, a further analysis concentrating on the relationship of biometric data processing and fingerprints with the fundamental rights guaranteed by the Charter in particular, will be completed in the ensuing chapter.

It is the opinion of the author of this thesis, that the collection of fingerprints from visa-exempt TCNs could be incongruous to Article 77 TFEU. The Article seeks to fulfil the Union objective of setting up an area of free movement of persons without internal border checks within the EU. The fact that the European Parliament and the Council of the European Union reason the processing of fingerprint data in the EES, and the provision of EUROPOL's access to such data on Article 77(2)(b) and (d) TFEU is counterintuitive, as the Treaty's scope on freedom of movement of persons does not extend to judicial cooperation.

[36] OJ C 326, 26.10.2012, Article 6(3).

2. EUROPEAN UNION CHARTER OF FUNDAMENTAL RIGHTS

The European Union Charter of Fundamental Rights (EUCFR), also known as the Charter, has served as a legally binding instrument of the Union since 2009, through the commencement of the TFEU, which infers that EU institutions and MS are bound to respect the EUCFR when they act within the scope of EU law.[37] Fundamental rights imply the intrinsic rights of the individual, and thus, cross traditional political boundaries[38].

The rights in the Charter guarantee individuals with the respect for core rights, on not only the traditional civil and political issues like freedom of expression and association, but also on 'second generation' aspects of an economic and social nature[39]. To this end, the Charter includes negative rights which impose a non-interference obligation upon the MS and the Union bodies[40], and positive rights which require positive action respectively, in order to respect and protect the core rights[41].

In line with Article 6(1) of TEU, the Charter constitutes a primary source of law in the EU, and is subject to the jurisdiction of the European Court of Justice (ECJ).[42] As an instrument, The Charter is the premier document protecting the fundamental rights of the individual in the European Union[43], with its basis on the European Convention on Human Rights (ECHR). The ECHR has set a threshold for level of protection, which the EU has acceded to in Article 6(2) of TEU[44].

[37] De Búrca, G. (2013). After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator? *Maastricht Journal of European and Comparative Law*. (20), p 169.
[38] Kenner, J. (2003). Economic and Social Rights in the EU Legal Order: The Mirage of Indivisibility. In: T. Hervey, J. Kenner (Eds.), *Economic and Social Rights under the EU Charter of Fundamental Rights* (1-25). Portland, Oregon: Hart Publishing, p 3.
[39] *Ibid.,* p 1.
[40] Zetterquist, O. (2011). The Charter of Fundamental Rights and the European Res Publica. In: G. Di Federico (Ed.), *Ius Gentium: Comparative Perspectives on Law and Justice 8,* (3-14). Dordrecht: Springer, p 3.
[41] Kenner, *supra nota* 38.
[42] Zetterquist, *supra nota* 40.
[43] *Ibid.*
[44] *Ibid.,* p 4.

Therefore, in addition to its position under the manifest of the jurisdiction of the ECJ, the Union has subjected itself to the jurisdiction of the European Court of Human Rights (ECtHR)[45].

2.1 Background

The Charter was drafted and adopted in 2000[46] to make the relevance of fundamental rights and their endorsement by the ECJ more visible to the EU citizens[47]. Initially, the idea to draw up a Charter arose from a decision taken by the European Council at the Cologne European Council in June 1999[48], accentuating the importance of protection of fundamental rights as a founding principle of the EU and its proviso for legitimacy within the *acquis*[49].

Between the years 2000 and 2009, the Charter held no legally binding force and remained at an uncertain stage, as it lacked an equal value and authority to EU Treaties[50]. After the coming-into force of the TFEU, and the commencement of binding force of the Charter, the Commission presented a new strategy for the effectual fulfilment of the rights enriched by the Charter. The Commission's communication document established that all proposals and interpretations of EU legislation must honour the Charter, and it is the Commission's task to monitor the compliance and application through its Annual Report[51].

2.2 The scope of application

According to case law of the Union, the right to protection of personal data is not an absolute right, however, it must be considered in relation to its function in society, thus, necessitating the preconditions of fair processing for specified purposes and legal basis[52]. The scope of application of the Charter is an issue of two separate subjects, whom are protected by its active personal scope

[45] Zetterquist*, supra nota* 44.
[46] De Búrca, *supra nota* 31.
[47] European Union, European Parliament. (1999). *Conclusions of the European Council in Cologne*, annex IV.
[48] C. McCrudden. (2001). *The Future of the EU Charter of Fundamental Rights*, chapter I.
[49] European Union, European Parliament, *supra nota* 47.
[50] González Fuster, G., Gellert, R. (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law, Computers & Technology*, 26 (1), p 74.
[51] European Union, European Commission. (2010). *Communication from the Commission on Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*, p 12.
[52] González Fuster, Gellert, *supra nota* 50, p 77.

and those under the passive personal scope, against whom the rights may be subjected to invoking[53].

2.2.1 The active personal scope

The scope of application of certain rights guaranteed by the Charter in the active personal scope diverge from protection for EU-nationals only to TCNs, and those universal rights which provide for every natural person falling within the scope of EU law or law of a MS[54]. The right to data protection for instance, is not limited by citizenship status and, thus, in the case of processing of fingerprint data of visa-exempt third country nationals, the right to data protection is enjoyed with equal protection through the active personal scope of the Charter.

The universal right to protection of fundamental rights is limited to the condition that the TCN falls within the scope of Union law or the law of one of its Member States[55]. In the case of visa-exempt TCNs, when traveling to and from the Schengen area, this group is covered by the Union law and therefore, benefit from the rights advocated by the Charter.

2.2.2 The passive personal scope

The passive personal scope of application of the Charter is defined through the horizontal direct effect of the provisions[56]. Article 51(1) of the Charter addresses the subjects of the non-interference obligation as all institutions and organs of the EU, and its MSs, in the event of implementation of the Union law[57]. The institutions in the provision refer to the European Parliament, the Commission, the Council and to the ECJ and the Court of Auditors, mentioned in Article 7 of the EC Treaty[58]. The previously referred to organs allude to the bodies of the Union which have been established by an EU Treaty[59], or in the case of the EES Regulation, have been assembled on the basis of a Treaty because legislation on the protection of personal data apply to such institutions[60].

[53] Curtin, D., van Ooik, R. (2001). The Sting is Always in the Tail: The Personal Scope of Application of the EU Charter of Fundamental Rights, *Maastricht Journal of European and Comparative Law*, 8 (1), p 103.
[54] *Ibid.*
[55] *Ibid*., p 104.
[56] *Ibid.,* p 105.
[57] OJ C 326, 26.10.2012, Article 51(1).
[58] Curtin, van Ooik, *supra nota* 56.
[59] *Ibid.*, p 106.
[60] OJ C 325, 24.12.2002, Article 286(1).

2.3. Competence of the EU in relation to Data Processing

The adoption of a right to data protection, distinct from the right to privacy, reflects the European Union's consideration of modern society and the need to protect such 'third-generation' fundamental rights. The successful compliance of the right to protection of personal data has an enabling function, and it thus, further contributes to the recognition of other fundamental rights and freedoms.[61]

Prior to the 2009 entry into force of the TFEU, the right to personal data protection was considered as a fundamental right in general, but it arose from different origins in comparison to today. The right to personal data protection in Europe arose from the right to privacy in Article 8 of the ECHR and was defined within EU framework in the Data Protection Directive. The Data Protection Directive had a double target for protecting the fundamental right to privacy and ensuring the free flow of personal data between MS.[62]

One of the leading cases in the process of developing adherence to the Charter, is the *Lindqvist* case[63], in which the ECJ in its decision voiced an emphasis on the issue that the Data Protection Directive's nature and the objective of balance between free flow of data, and protection of personal data, gives Member States a margin for manoeuvre in maintaining or introducing rules to attain the objective of the Data Protection Directive[64], which would give reason for the development of the GDPR. The ECJ, in its *Lindqvist* decision, interpreted the Data Protection Directive as a means to govern the fundamental right to privacy only, ruling out the existence of the right to data protection as a fundamental right, and thus, the problematic ruling gave rise for the weakening of the scope of right to data protection, as all intrusions to protection of personal data would be evaluated through mirroring of the right to privacy if the data was disclosed to third parties[65].

[61] M. Oostveen., K. Irion. (2016). *The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?*, p 3.
[62] González Fuster, Gellert, *supra nota* 50.
[63] *Ibid.*
[64] Court decision, 6.11.2003, Lindqvist, C-101/01, EU:2003:596, point 9.
[65] Tzanou, M. (2017). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-terrorism Surveillance.* Portland: Hart Publishing, p 51.

3. ANALYSING ARTICLE 8.2 OF THE EUROPEAN UNION CHARTER OF FUNDAMENTAL RIGHTS

The right to protection of personal data is recognised in Article 8 of the EU Charter, with its first paragraph recognising the right of all individuals to have protection of personal data considering themselves, within the Union. The provisions on the protection of personal data, in general, define the instances and conditions under which the personal data processing activities remain legitimate. Advocate General Siegbert Alber, in their Opinion, highlighted the necessity of data protection law, as there is no general prohibition of information disclosure[66].

For the purposes of this thesis, this chapter will analyse to which extent the processing of biometric fingerprint data in the EES of TCNs adheres to the standards set out in the second paragraph of the Article 8, providing that 'such personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law'[67]. The right of access to data and the right to have the data rectified will also be discussed with regard to the processing of fingerprint data in the EES.

3.1 Rights of the individual

The ECJ, in its case law, has noted that the right to data protection documented in Article 8 of the Charter does not constitute an absolute right, but rather, should be examined with respect to its function in society[68]. However, the elevation of the right to data protection to an EU-fundamental right in 2009, as discussed in the previous chapter, has brought about major advancements to the

[66] European Union, Court of Justice of the European Union. (2000). *Opinion of Mr Advocate General Alber in The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher,* point 41.
[67] OJ C 326, 26.10.2012, Article 8(2).
[68] Court decision, 9.11.2010, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen, C-92/09 and C-93/09, EU:C:2010:663, point 48.

level of protection for individuals subjected to processing of personal data within the Union framework[69].

The Advocate General Kokott, in the *Promusicae* case and proceedings before the ECJ, in their opinion noted, that the data subject, in the event of limitation to the right of data protection through disclosure to third party, should be able to foresee the purpose for which their data will be processed[70]. After the failure of the ECJ to recognise the right to protection of personal data, the *Promusicae* case was *de facto* the earliest judgment where the ECJ recognised the data protection as a fundamental right cherished in the Article 8 of the Charter, prior to the entry into force of the TFEU[71].

Wording in Article 8(2) of the Charter is quite ambiguous in specifying that data subjects shall have access to their data and a fundamental right to have inaccurate data rectified[72]. Thus, the Article fails to directly consider whether it includes the right of individuals to have their data erased.

The right of erasure to personal data has evolved into the concept of a right to be forgotten, where, the data should be as easy to withdraw as it is to give, as provided in the EU data protection law. The EES regulation, however, administers in its provisions, that the MS are responsible for informing the data subjects of their right to erasure of data in case of unlawful processing[73]. The right to be forgotten, as such, appears inapplicable in this context, but its relationship to the present regulation will be discussed in relation to the processing of biometric data of TCNs in the next chapter on legitimate justifications.

According to the right to data protection in Article 8(2) of the Charter, the data can only be kept for as long as necessary. The EES holds fingerprint data records of all TCNs traveling to and from the Schengen area, for the minimum period of three years and one day. As biometric data is sensitive data, the question arises, whether this duration exceeds the necessity and turns into

[69] González Fuster, Gellert, *supra nota* 50, p 73.
[70] European Union, Court of Justice of the European Union. (2007). *Opinion of Mr Advocate General Kokott in the Promusicae* case, point 53.
[71] Tzanou, *supra nota* 65, p 50.
[72] OJ C 326, 26.10.2012, Article 8(2).
[73] OJ L 327, 9.12.2017, Article 50(1)(h).

illegitimate. This question will be further discussed and analysed in the following chapters through case law of the Union.

All data subjects in the EU have a right to receive information on their data which is being processed, through the positive obligation of the data controllers. In a general EU level, this right is provided by the GDPR, however, the EES Regulation also recognises the right of TCNs, as data subjects, to information on the recording of their data[74]. The obligation to provide information to the visa-exempt TCNs, shall be fulfilled in written form and by the use of physical materials, such as, leaflets or posters or suitable electronic channels[75].

3.2 Legitimate objections and justifications

The activities of obtaining and processing fingerprints, for the fingerprint databases, by EU Member States, in order to adhere to their own obligations, may in fact contravene multiple fundamental rights guaranteed by the Charter[76]. Article 8(2) of the Charter identifies clearly and definitely, besides the definition of Article 5(1)(b) of the GDPR, that personal data shall be processed only for specified explicitly defined purposes and must not be further processed for other purposes without consent[77]. In the case of third country nationals without the requirement for visa, traveling within the Schengen area, the fair processing means that before preventing entry, an effective opportunity must be afforded to the passenger, allowing them to comply with the requirement to provide their fingerprint data[78].

Travel between the Schengen area and third countries is a voluntary action, therefore, the consent provided must be given freely and without duress. The means and manner through which consent from the passenger is gathered, is of extreme significance when discussing the legitimacy of processing of fingerprint data of the visa-exempt TCNs. When acquiring fingerprints from third country nationals for processing purposes, it is imperative, that this acquisition is not done through the administering of physical or psychological force, which results e.g. in forcing a person to place their hand onto the fingerprint scanner against their will. Forcibly collecting the fingerprints of

[74] OJ L 327, 9.12.2017, recital 43.
[75] *Ibid.*
[76] European Union, European Union Agency for Fundamental Rights. (2015). Fundamental Rights Implication on the Obligation to Provide Fingerprints for Eurodac, p 4.
[77] OJ C 326, 26.10.2012, Article 8(2).
[78] European Union, European Union Agency for Fundamental Rights, *supra nota* 76.

TCNs is to be avoided, as it diminishes the risk of a violation of fundamental rights[79], especially the principle of fair processing expressed in Article 8(2) of the Charter, as in this case it can be assumed that the use of force is not provided for by national law.

In order to satisfy and comply to the principle of lawful processing, it is paramount that the data subject is informed by the officers of the national authority, both orally in a mutually intelligible language, and in writing, of the necessity to provide fingerprints in order to travel to the Schengen area[80]. It is also critical, that the officers advise the data subject of the purposes for the processing in accordance with Article 13 of the GDPR. Finally, it is essential, that the passenger is informed of the ramifications if they refuse to supply their fingerprint data[81].

With an increase in the usage of technology and IT systems, in fighting against irregular migration and terrorism, the data may be subjected to other processing activities falling outside of the originally intended and justified processing methods.[82] In cases of interoperability between IT systems, in particular, the aforementioned risk is substantial[83], and given the cooperation of the EES and other systems, principally, the aforementioned risk of violation of fundamental rights is substantial, and given the cooperation between the EES and other systems, the risk must be acknowledged. The Regulation 2017/2226 defines numerous actors with the authority to access the data stored in the EES database, making it possible for the data to be shared to private persons or third countries. The main purpose of the EES is to register entries and exits of TCNs, but it is additionally designed to combat serious crimes and terrorism, therefore, illegal access and hacking threats to the system are a genuine concern. It is the opinion of the author that importance on the lawful sharing must be stressed and the minimisation of persons with access must be given further inspection.

In the event that a passenger abstains from consenting to the collection of their fingerprint data, the national authorities will invoke a legitimate basis laid down by law for the legality of the processing, which is derived from the previously mentioned TFEU Article 77. However, for the purposes of this thesis, an evaluation on the validity of the cited legitimate legal basis is irrelevant,

[79] European Union, European Union Agency for Fundamental Rights*, supra nota* 76, p 2.
[80] *Ibid.*, p 4.
[81] *Ibid*.
[82] European Union, European Union Agency for Fundamental Rights. (2018). *Under watchful eyes: Biometrics, EU IT systems and Fundamental Rights*, p 13.
[83] *Ibid.*

and thus, the following paragraphs will focus on the protocols of the EES in the enforcement process of the rights of the data subjects with regard to their fingerprint data.

Regardless of the fact that the Charter does not guarantee the right to data erasure, hereinafter referred to as the right to be forgotten, the EES Regulation accomplishes to fulfil the data controller's obligation to guarantee the data subject with the present right, through the application of Articles 15 to 18 of the GDPR[84]. Visa-exempt TCNs, whose fingerprints are recorded in the border-crossing process, have a right to file requests concerning their rights derived from the Charter, and the data protection legislation to the competent authority of any MS, and are pledged to receive a response within 45 days[85]. Given that the request considers the right of rectification or erasure of fingerprint data, the authorities of the MS are responsible to investigate the lawfulness of the processing within 30 days of receiving such request[86].

The right to be forgotten in the context of the EES Regulation, however, does not produce an absolute right per se, as only unlawfully recorded fingerprint data, perchance, could be erased as a result of a request from the data subject[87]. In the event that the national authorities do not agree with the claim of unlawfully processed, or verity and accuracy of fingerprint data, the MS is to provide a written explanation of the decision to the affected TCN[88]. This information illustrates, in addition, to why the authorities in the MS will not amend or remove the personal data or curb the processing, also the possible alternative actions they can employ, e.g. lodging a complaint before the court[89], if in disagreement with the decision of the national authorities.

3.3 Legal precedents

In the landmark *Google v. Spain* judgment, the ECJ affirmed the existence of a right to have personal data deleted from search engines on request, despite the fact that the publication of personal data on the website of the magazine was permitted by law[90]. This decision evolved to the

[84] OJ L 327, 9.12.2017, recital 59.
[85] *Ibid.*, Article 52(1).
[86] *Ibid.*, Article 52(2).
[87] *Ibid.*, Article 52(3).
[88] *Ibid.*, Article 52(4).
[89] *Ibid.*, Article 52(5).
[90] Korpisaari, P., Pitkänen, O., Warma-Lehtinen, E. (2018). *Uusi Tietosuojalainsäädäntö*, Helsinki: Alma Talent, p 226.

birth of the recognition of the right to be forgotten from the Data Protection Directive[91]. In the ruling on 13th May 2014, the ECJ contrasted the Data Protection Directive and Charter of Fundamental Rights as both influential to its decision, however, the judgment did not go deep into the content of, for example, the right to protection of personal data (Article 8 of the Charter) and to the extent of protection it offers, and therefore, fails to define the reach of right to be forgotten[92]. The court did address the fundamental right to protection of data as a legal basis for a claim to have personal data deleted, but the ECJ was very minimal in justifying fundamental rights as a reasoning, and failed to interpret the reach of the right and define it in the light of the circumstances of the case, as well as explain and justify how the operation of Google is also likely to infringe Article 8[93].

Despite Google's position as a private internet operator, and the EES being a Union IT-database, where the data is not available to the general public, the discussed case law appears to present the EU, both in its legislative and judicial authorities, in a negative way as the definitions of Article 8 of the Charter remain equivocal.

Advocate General Campos Sánchez-Bordona, in their opinion published in the ECJ's fourth press release of 2020, in recent cases from France, Belgium and the United Kingdom, has stressed that the tactics and approaches used when encountering terrorist activity must be consistent to the stipulations laid out by the rule of law[94]. From the opinion it can be derived that the exercise of mass surveillance of the MS's national authorities is legitimate as long as they do not commission private entities to take part in those processes[95].

The principle of fair processing, guaranteed by the Charter, can be seen as including the step to arrange the storage period of the personal data for only as long as it is necessary[96], which should be balanced with the purpose of processing and applicable legal obligations[97]. The standard for

[91] Post, R. C. (2018). Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere, *Duke Law Journal*, 67 (5), p 981.
[92] Frantziou, E. (2014). Further Developments in the Right to Be Forgotten: The European Court of Justice's Judgment in the Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos, *Human Rights Law Review*, 14 (4), p 768.
[93] *Ibid.*
[94] European Union, Court of Justice of the European Union. (2020). *Advocate General's Opinions in Case C-623/17 Privacy International, Joined Cases C-511/18 La Quadrature du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Other,* p 1.
[95] *Ibid.*
[96] OJ L 119, 27.4.2016, recital 39.
[97] *Ibid.*, Article 5(1)(e).

compliance with this rule, found in the GDPR, however, remains unspecified both in the present regulation, the absence of a new data retention legislation and in the Union's case law.

In the EES, the minimum period for which fingerprint data may be retained is 3 years and one day[98]. This timeframe will be extended in the event of new entries and exits to the Schengen area after the initial records[99]. The legitimacy of the retention period of fingerprint data in the EES must be evaluated through its objectives and function in the society. Taking into account the Union's objective of combating terrorism, crime and irregular migration, the three-year retention period seems justifiable given the presumption of a single visit or alternatively an extension of three years and one day in case of revisit to the Schengen area.

[98] OJ L 327, 9.12.2017, *supra nota* 28.
[99] *Ibid.*

4. ANALYSING ARTICLE 8.3 OF THE EUROPEAN UNION CHARTER OF FUNDAMENTAL RIGHTS

Article 8(3) of the Charter expresses the supervision of the protection of personal data, by an independent authority, as an integral constituent for the protection of individuals[100], in respect of the processing of personal data. The importance of monitoring personal data processing activities by a national independent authority is also embedded in other areas of primary law of the EU, namely in Article 16(2) TFEU.[101] The Article therefore attributes a guardian of fundamental rights and freedoms status upon these supervisory authorities with regard to the processing of personal data[102].

4.1 Definition of independent authority

The processing of fingerprint data by national authorities in the EES is subjected to control by an independent authority, which each MS is to designate under the rules of the GDPR, whereas the actions of the Union and its bodies, as a whole, shall be reviewed by the European Data Protection Supervisor[103]. The absolute independence of national authorities in performing their monitoring tasks is a prerequisite to the administration of a high level of protection of personal data[104], which, in the case of processing fingerprints of TCNs, requires the national supervisors to remain independent of the processing activities, and hence, the transnational interest and factors of the system together with the aims of the Charter, to cooperate with other MS' authorities and with the Commission[105]. To this end, taking into account that the fingerprint data stored in the system is of persons not suspected of having committed any crimes, the freedom from external influence or

[100] Court decision, 9.11.2010, European Commission v Federal Republic of Germany, C-518/07, EU:C:2010:125, point 23.
[101] European Union, Court of Justice of the European Union. (2013). *Opinion of Mr Advocate General Wathelet in Commission v Germany,* point 65.
[102] *Ibid*.
[103] OJ L 327, 9.12.2017, recital 41.
[104] OJ L 119, 27.4.2016, recital 117.
[105] *Ibid.*, recital 118.

instruction of the independent authorities is necessitated and their members cannot engage in other placements or operations, which are irreconcilable to the interests of the independent authority[106].

In the interest of adhering to the demands of the fundamental rights guardian, the national authorities must possess effective, investigative powers to access information requiring human, technical and financial resources in addition to an interference capacity designed to limit and inhibit any processing activities contrary to the principles of fair processing. It is also of paramount necessity, that the supervisory authority accepts complaints lodged by persons concerned per their right to enforce the rights of the data subject in the last subparagraph of the Article 50(1) of the EES Regulation.[107]

Access to sensitive personal data in the EES constitutes a limitation on the right to protection of personal data[108], and therefore, the extent of the enforcement of this limitation must comply with the principles of necessity and proportionality. The national authorities, with access to information in the EES, comprise of the border authorities supplying the border checks, the police and EUROPOL authorities, together in fighting against serious crime and terrorism and the police authorities on their own in combating irregular migration, and in extreme cases the national immigration authorities may have access to the data stored in the EES in the enforcement of return procedures[109]. In addition to the aforementioned, the EES Regulation allows access to a limited portion of data in the system by private persons, e.g. airline carriers for the controlling of visas[110]. In this case, it must be acknowledged, that despite the non-applicability of visa controls by carriers to the visa-exempt TCNs, it is essential that the access is limited only to authorised staff working for the carrier.

4.2 Legal precedents

As a result of the rise in perceived threats to security during the 21st century, national law enforcement officers have escalated their access to national databases[111]. Despite the fact that this

[106] *Ibid.*, Article 52.
[107] Bieker, F. (2016). Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice. In: A. Lehmann, D. Whitehouse, S. Fischer-Hübner, L. Fritsch, C. Raab (Eds.), *Privacy and Identity Management. Facing up to Next Steps. Privacy and Identity 2016* (125-139). Cham: Springer, p 126.
[108] European Union, European Union Agency for Fundamental Rights, *supra nota* 82, p 64.
[109] *Ibid.*, p 61.
[110] OJ L 327, 9.12.2017, Article 13.
[111] European Union, European Union Agency for Fundamental Rights, *supra nota* 108, p 66.

thesis does not intend to analyse the national authorities, given that the national police forces have access to the data stored in the EES, it is important to take into account issues regarding misuses of authority reported to the Union by the national officials, with regard to similar JHA IT databases. The Italian and Belgian officials have reported that the personal data in the European Asylum Dactyloscopy Database (EURODAC) and VIS system databases have been unlawfully converted into additional tables and forwarded to the use of other law enforcement authorities[112].

To prevent misuse of right to access, the EES seeks to limit the authorities with access to the merest, and due to extreme necessity, access is limited through the safeguard *cascading system*, which prevents unproportionate law enforcement access to the IT system. Consistent with this safeguard, the authorities are to search information from the system in question, if a precursory check in other MS's national databases or fingerprint databases, which is possible via the Prüm system, has not been fully completed within two days of commencement. Given that some of the persons of whom the EES records fingerprint data may be linked to terrorist activity and serious crime, the *cascading system* is in place to make sure that in criminal cases, the principle of proportionality materialises through the obligation to search other databases which are more closely related to criminal investigations.[113]

4.3 Case studies

In the earliest case law from the European Court of Justice, on the role of the supervisory authority in *European Commission v Germany*, the Court concluded that in addition to the total independence from the subjects of supervision, the authorities must refrain from any pressure directed, either directly or indirectly, from any other origin, because any political influence affecting the monitoring task of the supervisory authorities is sufficient to hinder their independence[114]. Given the unique role of the supervisory authorities, acting as an auditor of the private and public authorities, whilst remaining independent from state powers, the ECJ held that any state scrutiny over the national supervisory authority is detrimental to the independence and freedom of external influence of the latter authority[115], and thus, forbidding the states to interfere

[112] *Ibid.*
[113] *Ibid*.
[114] Court decision, 9.11.2010, *supra nota* 100, point 36.
[115] Court decision, 9.11.2010, *supra nota* 114, point 37.

or guard the interest of companies in the private sector[116]. In this context, it is necessary to employ a more extensive research into the nature and qualities of the supervisory authority, which in the case of the EES are the national law enforcement authorities.

The Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the MS of the EU, defines a law enforcement authority as a national police or customs authority, or other authority permitted by national law in the MS, to avert and scrutinise criminality and related activities and to exert control and coercive measures in the context of such nefarious acts[117]. Notwithstanding the definition, the selection of competent national authorities responsible for the fulfilment of the role of the law enforcement authority, as set out in the Framework Decision, vary from country to country[118].

When assessing whether the access of national law enforcement bodies to the data stored in the EES complies with the principle of independent supervisory authority, it is important to note that the provision excludes national security agencies from the sphere of law enforcement authorities[119]. As reported by the Council in their 2009 Guidelines on the application of the Framework Decision 2006/960/JHA, most MSs show to have nominated police forces as the prioritised force[120]. There are, however, countries which have, in addition to the aforementioned, appointed prosecutors' offices, military and customs authorities, tax authorities or ministries and special directorates in ministries to the law enforcements authority's role[121]. Thus, in the context of overseeing the processing of personal data in the EES databases in the Member States, there are substantial differences as to the nature and appearance between the national supervisory authorities.

It could be derived from the discrepancies in law enforcement authority nominations across the Union Member States, that the independency of authorities in certain countries, i.e. directorates in ministries, from the State could prove equivocal. The EES Regulation requires the access to

[116] Bieker, F., *supra nota* 107, p 127.
[117] OJ L 386, 29.12.2006, Article 2(a).
[118] Carrera, S., González Fuster, G., Guild, E., Mitsilegas, V. (2016). *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*. Brussels: Centre for European Policy Studies, p 8.
[119] OJ L 386, 29.12.2006, *supra nota* 117.
[120] Carrera, González Fuster, Guild, Mitsilegas, *supra nota* 118.
[121] European Union, Council of the European Union. (2009). *Guidelines on the Implementation of Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union*, annex III.

information in the database to be narrowed down to only such authorities who are responsible for the prevention, detection or investigation of terrorist offences or other serious criminal offences, and those monitoring the lawfulness of the processing[122] and, therefore, the compatibility of tax authorities alone could be arguable.

[122] OJ L 327, 9.12.2017, recital 23.

5. ANALYSING ARTICLE 52 OF THE EUROPEAN UNION CHARTER OF FUNDAMENTAL RIGHTS

The objective of Article 52 of the Charter is to define the scope of its principles and rights and to set guidelines on the interpretation of those rights.[123] The EES Regulation has committed to respect the fundamental rights guaranteed by the Charter[124], and thus, this chapter will seek to analyse the extent to which it follows the scope of validity in limiting the right to data protection. Despite the existence of the limitation, all other requirements related to the protection of personal data stemming from the GDPR are adhered to[125].

In the first paragraph of Article 52 of the Charter, the limitation of fundamental rights is restricted to legally enforced purposes, subjected to the principle of proportionality, corresponding to the objectives of the general interest of the Union[126]. The phraseology of the article is derived from a decision in the case *Kjell Karlsson and Others*, where the ECJ conceded that proportionate restrictions on the enforcement of fundamental rights over the public interest are not a constraint upon the rights[127]. Given the legal basis of the processing activities of biometric data from visa-exempt third country nationals is in the EES Regulation, the following sections of this chapter shall focus on assessing to what degree the limitation complies with the principle of proportionality and what needs to be taken into account when limiting the fundamental right to data protection.

[123] Peers, S., Hervey, T., Kenner, J., Ward, A. (2014). *The EU Charter of Fundamental Rights: A Commentary*. Oxford: Hart Publishing, p 1455.
[124] OJ L 327, 9.12.2017, recital 59.
[125] *Ibid.*
[126] Peers, Hervey, Kenner, Ward, *supra nota* 123.
[127] *Ibid.*

5.1 Principle of proportionality

Proportionality, as a general principle of law[128], serves as a tool which allows for the production of resolutions, through the weighing of two comparatives in the process of determining the prevailing interest[129]. The principle of proportionality can be used to see if a limitation to a fundamental right is legitimate, and in this case, protecting the public interest. However, there are certain fundamental rights which transcend the possibility of limitation. These absolute fundamental rights extend to include the maintenance of human dignity and the prohibition of torture[130].

As developed in aforementioned chapters of this thesis, the processing activities of the biometric data of visa-exempt TCNs is an actual limitation on the data subjects' fundamental right to data protection. Thus, a proportionality test is required to ascertain whether the practices are incompatible with the meaning of Article 52 of the Charter. If any incompatibilities with the principle of proportionality are discovered, the research shall determine what measures are in place to ensure conformity of the fingerprint processing activity with respect to the principle of proportionality.

The proportionality test consists of three defined measures reflecting the suitability, necessity and the *stricto sensu* compliance of the purportedly incompatible limitation[131]. In determining the suitability of the processing activities of fingerprint data of visa-exempt TCNs traveling within the Schengen area, the ability of the EES to fulfil the Union objective of combatting serious crime and terrorism should be assessed from the relevance-focussed point of view. Given the parameters of the complexity of preventing terrorism and serious crime and the tracking-enabling function of the system, it is the opinion of the author, that the limitation on the discussed right manifests the safeguarding-objective appropriately.

For the necessity of the measures it is important that there are no alternative ways to achieve the goal that are less inhibitive as to the individuals' fundamental right to data protection[132]. The system allows for the tracking of visa-exempt TCNs, however, the tracking of data subjects is not

[128] Harbo, T. (2010). The Function of the Proportionality Principle in EU Law, *European Law Journal*, 16(2), p 159.
[129] Andenas, M., Zleptnig, S. (2007). Proportionality: WTO Law in Comparative Perspective, *Texas International Law Journal*, 42 (3), p 375.
[130] European Union, European Commission, *supra nota* 51, p 5.
[131] Harbo, T., *supra* nota 128, p 165.
[132] *Ibid.*

systematic, as the national authorities will only be notified in the event of individuals exceeding their authorised stay and the recorded information on the personal file, fingerprints in this instance, shall only be employed in the aid of criminal investigations. On the other hand, there is a possibility that a person could become suspected of a crime due to profiling, similarities in name with other data subjects or erroneous data entries in the system and subsequently having to prove their innocence[133]. Despite this possibility for mistakes, other methods of controlling serious crime and terrorism are more restrictive, resulting in either limits on or complete prohibition of the movement of TCNs to and from the Schengen area. Consequently, the author concludes that the establishment of the EES data system and its related data processing activities do present the less restrictive option as per the objective of the Union, therefore passing the necessity test.

The *stricto sensu* assessment stipulates that even if the measure is suitable and necessary, a resolution cannot be considered proportionate if it imposes an inordinate encumbrance upon the data subject[134]. The providing of fingerprint data requires the passenger to place fingers onto a fingerprint scanner, thus, not requiring any prior preparations by the data subject. Hence, it is the opinion of the author of this thesis, that the presentation of fingerprint information to the authorities is to be regarded as an additional step to identification along with facial recognition and non-biometric passport data check and, therefore, does not constitute an unnecessary burden within the definition of *stricto sensu*. Moreover, the obligation to provide biometric data for traveling within the Schengen area is free from misinterpretations, as in the EES Regulation 2017/2226 it is coded in clear and understandable language, therefore, removing a threat of unforeseeability at the border crossing points.

5.2 Legal precedents

The EU and Canada had envisaged a Passenger Name Record (PNR) to transfer personal data of passengers electronically prior to the entries into Canada, thus, enabling the national authorities to monitor the passengers and to detect any security threats[135]. The procurement of PNR data was required by the Canadian government from all air carriers[136], and the EU viewed this as a way for

[133] European Union, European Union Agency for Fundamental Rights, *supra nota* 82, p 65.
[134] Harbo, T., *supra nota* 128, p 165.
[135] European Union, Court of Justice of the European Union. (2017). *Opinion 1/15 of the Court (Grand Chamber)*, point 21.
[136] *Ibid.,* point 14.

the MSs together with the EUROPOL and Eurojust to co-operate with the Canadian judicial authorities in the fight against terrorism and serious transnational crime[137].

The ECJ found the proposed PNR agreement between the EU and Canada contradictory to the principle of proportionality due to lack of provisions for the legitimacy of transfer and retention of sensitive personal data[138]. It is the opinion of the author of this thesis that, despite the draft of a PNR exchange between Canada and the EU would not have contained data of biometric identifiers, the fundamental idea of the system was similar to the one of the EES, in recording the border crossing points together with sensitive personal data. However, this is where the similarities end, due to the fact that the EES Regulation contains the provisions on retention of personal data which the ECJ appears to consider as preconditions to proportionality.

It could be derived from Union case law in the *Omega* case*,* that the ECJ will only allow the employment of the least restrictive measure as proportionate before the procedural choice. Considerations of alternative options are not publicly recorded, therefore, it has not been possible for the author of this thesis to analyse, whether, in light of the *Omega* case, the processing of fingerprint data in the EES was the only option considered by the EU, and declared the least restrictive measure in achieving the aim of combating terrorism, irregular migration and serious crime.

Keeping in mind the principle of the least restrictive measure, different considerations for the recording of fingerprints in the EES must be analysed. In the *Schwarz* case, considering the processing of fingerprints of an individual, the ECJ recognised that the only alternative for fingerprint scanning is an iris scan, which for the purposes of identification does not present a less restrictive alternative[139]. The Court, thus, deemed the employment of fingerprint scanning as a measure, despite it not being able to prevent entries of unauthorised persons, as proportionate to the aim of preventing nefarious use of passports, because it significantly reduced the possibility of such persons being able to cross borders[140].

Despite the fact that the *Schwarz* case concerned an application on the proportionality of fingerprint collection in the process of issuing national passports, the cases are comparable, as in

[137] European Union, Court of Justice of the European Union, *supra nota* 135.
[138] *Ibid.*, point 232.
[139] Court decision, 17.10.2013, Michael Schwarz v Stadt Bochum, C-291/12, ECLI:EU:C:2013:670, point 51.
[140] *Ibid.*, point 43.

both instances fingerprints are recorded for the purpose of preventing unauthorised entries within the EU together with the Schengen area, and, on a more abstract level, the objective of combating irregular migration. In the opinion of the author, when managing the prevention of illegal migration of the TCNs into the EU, the ECJ's ruling is applicable to the EES, because biometric identifiers are paramount to the preventative measures required to ensure no admittance on falsified documentation occurs. In the context of the two aforementioned cases, the processing of fingerprint data of TCNs traveling to and within the Schengen area should be considered as the less constrictive measure in combating irregular migration. Therefore, the provision on processing fingerprint data in Article 17 1.(c) is in pursuance to one of the objectives of general interest in the EU.

5.3 Case studies

In the landmark *Digital Rights Ireland* case, which paved the way for the creation of the GDPR, the ECJ noted that the fundamental right to data protection is not an absolute right and interferences with that right could be justified when pursuing legitimate aims to fight serious crime and terrorism[141]. Hence, the settled concept of justice that contributions to fight against terrorism[142] and serious crime[143] ultimately correspond to the interest of public security, the ECJ concluded that the allowance of competent national authorities' access to the personal data, in accordance to the then effectual Data Retention Directive, satisfied the objective of general interest[144]. However, the data processing activities contained within the *Digital Rights Ireland* case did not satisfy the requirements stemming from the right to data protection. Furthermore, the Court declared the Data Retention Directive regulating such retention of personal data as invalid on the ground of, *inter alia,* dissatisfaction with the proportionality requirement in respect to Articles 8 and 52 of the Charter[145].

[141] Court decision, 8.4.2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, C-293/12 and C-594/12, EU:C:2014:238, points 41-44.
[142] Court decision, 3.9.2008, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, C-402/05 P and C-415/05 P, ECLI:EU:C:2008:461, point 363.
[143] Court decision, 23.11.2010, Land Baden-Württemberg v Panagiotis Tsakouridis, C-145/09, ECLI:EU:C:2010:708, points 46-47.
[144] Court decision, 3.9.2008, *supra nota* 141, point 44.
[145] *Ibid.*, point 71.

Given that the aims of the then enforced Data Retention Directive, under the objective of public interest, with regard to the storage of personal data and the access of national authorities to the aforesaid data[146], were found to contradict the principle of proportionality, it is noteworthy to consider that the EES however, does not purposely collect data of persons directly or indirectly connected to criminal activities or investigations. Therefore, the two cases are not comparable, as the law enforcement objective of the EES does not correspond to that in the *Digital Rights Ireland* case. As discussed in the previous chapter, in the event of criminal investigations, the *cascading system* in the EES, compels the law enforcement authorities of the MS to initially consult the national databases containing fingerprint records. This practice is of utmost importance owing to the way it limits the authority of the law enforcement bodies, and thus, contributes towards compliance of the proportionality principle[147].

[146] OJ L 105, 13.4.2006, Article 8.
[147] European Union, European Union Agency for Fundamental Rights, *supra nota* 82, p 67.

CONCLUSION

The EES was established to identify and record all individuals staying in the Schengen area, with the objective of combating serious crime, terrorism and irregular migration, however, for the purposes of this thesis, only visa-exempt TCNs traveling to, and from, the Schengen area were taken into consideration. The system notifies national authorities when the duration of the authorised 90-day stay has expired, based on the collection of the date, time and place of entries and exits of TCNs, automatically calculating the duration of authorised stay. Individual files of TCNs will be stored in the EES for a period of three years and one day, which could be extended by a further duration upon re-entrance.

The aim of this research was to assess and evaluate the degree of infringement on the fundamental right to data protection, as a result of processing of fingerprint data from TCNs traveling within the Schengen area. The issue of possible implications on the fundamental rights, enriched by the Charter, is framed by the hypothesis that the collection and storage of biometric data is incongruous to the principles of fair processing and proportionality laid down in Article 52 of the EUCFR.

Discrepancies between the objectives, implementation and effects of the measure, and, legislation, relevant cases and precedents are identified, then contrasted against the principle of proportionality. The findings indicate, that the practice of collecting biometric fingerprint data from nationals of third countries, does not introduce a direct impact on the fundamental right to data protection, but nevertheless, does however amount to a significant limitation on the individual's right to data protection. Legality of the constraint is, on the contrary to the hypothesis of this thesis, found to be proportionate due to its basis on the facilitation of the identification of persons enjoying the visa waiver, and thus, contributing to the fight against the challenges of falsified documentation and identity fraud, and more extensively, to prevent terrorism, irregular migration and serious crime.

In this thesis, an impact assessment has been conducted, in addition to assessing the necessity and proportionality of the measures, a weighing of alternative identification options against the infringement on fundamental rights has been undertaken. Through extensive qualitative research, another factor in support of the proportionality of fingerprint processing in the EES is, that alternative solutions targeted at issues that are in the public interest, such as, illegal migration, terrorism and international crime, would result in increased restrictions on the individuals at the border-crossing, and thus, the handling of biometric data, in light of Union case law, is to be regarded as the least restrictive measure.

While it is true, that individuals may suffer as a result of the possible unlawful reprocessing, the assumption of unauthorised additional data usage by law enforcement authorities would result in an unproportionate assertion, and furthermore, in the opinion of the author, would contradict the principle of rule of law. To ensure the proportionality in the utilisation of personal data, the EES has also employed safeguards, such as the *cascading system*, to deter the competent authorities from engaging in such malevolent acts.

Despite having disproven the hypothesis, the author of this thesis will conclude with further developments intended to contribute to consistency in the implementation of EU law. Firstly, as demonstrated by this research, the MSs have different approaches as to the application of certain definitions, therefore, it is the opinion of the author of this thesis, that, from the point of view of fair processing of data, the Union should establish a pre-defined definition for a 'law enforcement authority' to ensure coherence across the Member States. Secondly, the findings from case law illustrate that the main right under discussion in this thesis, Article 8 of the Charter on the right to data protection, is unclear as to the full extent of protection that it offers, and thus, the level of protection should be further defined, e.g. with clauses on modern-age manifestation of personal data. Thirdly, the TFEU Article 77, which defines how to Union may develop policies on movement and immigration into the EU, does currently not extend the jurisdiction to judicial co-operation, and therefore, an alteration should be placed in order to guarantee the solidity of the legal basis for the EES.

Following the research conducted in this thesis, the author proposes the subsequent contributions to the discourse; assessment of the challenges of the Smart Borders Package in relation to the right to privacy, as provided in Article 7 of the Charter, and the right to non-discrimination in Article 21 of the EUCFR, because it is clear that profiling takes place, through biometric identification

technology such as facial recognition and fingerprint scanning, in the IT systems which monitor movement in the Union via the use of passenger records.

Despite the establishment of a lawful limitation on the fundamental right to data protection, the EU border management is subject to the complexity of having multiple, sometimes interoperable, IT systems. These systems have not aided comprehension among the data subjects, and thus, without further clarification on the relationship between the centralised and decentralised IT systems, the uncertainty will only continue.

LIST OF REFERENCES

Scientific books

1. Bossong, R., Carrapico, H. (2016). *EU Borders and Shifting Internal Security: Technology, Externalization and Accountability.* Cham: Springer.

2. Carrera, S., González Fuster, G., Guild, E., Mitsilegas, V. (2016). *Access to Electronic Data by Third-Country Law Enforcement Authorities: Challenges to EU Rule of Law and Fundamental Rights*. Brussels: Centre for European Policy Studies.

3. Korpisaari, P., Pitkänen, O., Warma-Lehtinen, E. (2018). *Uusi Tietosuojalainsäädäntö*, Helsinki: Alma Talent.

4. Peers, S., Hervey, T., Kenner, J., Ward, A. (2014). *The EU Charter of Fundamental Rights: A Commentary*. Oxford: Hart Publishing.

5. Schwab, K. (2017). *The Fourth Industrial Revolution*. Redfern: Currency Press.

6. Tzanou, M. (2017). *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-terrorism Surveillance.* Portland: Hart Publishing.

Scientific articles

7. Andenas, M., Zleptnig, S. (2007). Proportionality: WTO Law in Comparative Perspective, *Texas International Law Journal*, 42 (3), 371-428.

8. Bieker, F. (2016). Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice. In: A. Lehmann, D. Whitehouse, S. Fischer-Hübner, L. Fritsch, C. Raab (Eds.), *Privacy and Identity Management. Facing up to Next Steps. Privacy and Identity 2016* (125-139). Cham: Springer.

9. Curtin, D., van Ooik, R. (2001). The Sting is Always in the Tail: The Personal Scope of Application of the EU Charter of Fundamental Rights. *Maastricht Journal of European and Comparative Law*, 8 (1), 102-114.

10. De Búrca, G. (1998) Principle of Subsidiarity and the Court of Justice as an Institutional Actor. *Journal of Common Market Studies*, 36 (2), 217-235.

11. De Búrca, G. (2013). After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator? *Maastricht Journal of European and Comparative Law,* (20), 168-184.

12. De Capitani, E. (2014). The Schengen system after Lisbon: from cooperation to integration. *ERA Forum,* 15, 101-118.

13. Frantziou, E. (2014). Further Developments in the Right to Be Forgotten: The European Court of Justice's Judgment in the Case C-131/12, Google Spain, SL, Google Inc v Agencia Española de Protección de Datos. *Human Rights Law Review*, 14 (4), 761–777.

14. González Fuster, G., Gellert, R. (2012). The fundamental right of data protection in the European Union: in search of an uncharted right. *International Review of Law, Computers & Technology*, 26 (1), 73–82.

15. Harbo, T. (2010). The Function of the Proportionality Principle in EU Law. *European Law Journal*, 16 (2), 158-185.

16. Jeandesboz, J. (2016). Smartening Border Security in the European Union: An associational inquiry. *Security Dialogue,* 47 (4), 292-309.

17. Jeandesboz, J. (2017). How to make sense of information and data processing. In: A. R. Servent, F. Trauner (Eds.), *Routledge International Handbooks,* Part III, Section 15. New York, USA: Routledge.

18. Kenner, J. (2003). Economic and Social Rights in the EU Legal Order: The Mirage of Indivisibility. In: T. Hervey, J. Kenner (Eds.), *Economic and Social Rights under the EU Charter of Fundamental Rights,* (1-25). Portland, Oregon: Hart Publishing.

19. Lwin, M. (2010). Privacy issues with DNA databases and retention of individuals' DNA information by law enforcement agencies: the holding of the European Court of Human Rights case S and Marper v. United Kingdom should be adapted to American Fourth Amendment jurisprudence. *Information & Communications Technology Law*, 19 (2), 189-222.

20. Nguyen, F. G. (2018). The Standard for Biometric Data Protection. *Journal of Law & Cyber Warfare*, 7 (1), 61-84.

21. Post, R. C. (2018). Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere. *Duke Law Journal*, 67 (5), 981-1072.

22. Schermer, B. W. (2011) The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27 (1), 45-52.

23. Sontowski, S. (2018). Speed, Timing and Duration: Contested Temporalities, Techno-political Controversies and the Emergence of the EU's Smart Border. *Journal of Ethic and Migration Studies*, 44 (16), 2730-2746.

24. Zetterquist, O. (2011). The Charter of Fundamental Rights and the European Res Publica. In: G. Di Federico (Ed.), *Ius Gentium: Comparative Perspectives on Law and Justice, 8,* (3-14). Dordrecht: Springer.

Handbooks

25. Bourbeau, E. (2017). *Handbook on Migration and Security.* Cheltenham, United Kingdom: Edward Elgar Publishing.

26. Maltoni, D., Maio, D., Jain, A. K., Prabhakar, S. (2009). *Handbook of Fingerprint Recognition.* (2nd ed.) London, England: Springer.

EU and international legislation

27. Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p 391-407.

28. Consolidated version of the Council Framework Decision on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p 1-89.

29. Consolidated version of the Treaty establishing the European Community, OJ C 325, 24.12.2002, p 33-184.

30. Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, p 13-390.

31. Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/56/EC, OJ L 105, 13.4.2006, p 54-63.

32. Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, OJ L 119, 27.4.2016, p 1-38.

33. Regulation 2017/2226 of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, OJ L 327, 9.12.2017, p 1-82.

Court decisions

34. Court decision, 3.9.2008, Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, C-402/05 P and C-415/05 P, EU:C:2008:46.

35. Court decision, 6.11.2003, Lindqvist, C-101/01, EU:C:2003:596.

36. Court decision, 8.4.2014, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, C-293/12 and C-594/12, EU:C:2014:238.

37. Court decision, 9.11.2010, European Commission v Federal Republic of Germany, C-518/07, EU:C:2010:125.

38. Court decision, 9.11.2010, Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, C-92/09 and C-93/09, EU:C:2010:663.

39. Court decision, 17.10.2013, Michael Schwarz v Stadt Bochum, C-291/12, EU:C:2013:670.

40. Court decision, 23.11.2010, Land Baden-Württemberg v Panagiotis Tsakouridis, C-145/09, EU:C:2010:708.

41. S. and Marper v. United Kingdom, no. 30562/04 and 30566/04, ECHR 2008.

Other sources

42. Bigo, D., Carrera, S., Hayes, B., Hernanz, N., Jeandesboz, J. (2012). *Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An evaluation of Current and Forthcoming Proposals.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2198802&download=yes, 30 January 2020.

43. C. McCrudden. (2001). *The Future of the EU Charter of Fundamental Rights*. Retrieved from https://jeanmonnetprogram.org/archive/papers/01/013001.html, 23 February 2020.

44. European Union, Council of the European Union. (2009). *Guidelines on the Implementation of Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union*. Retrieved from https://www.statewatch.org/news/2009/apr/eu-council-swedish-iInitiative-guidelines-8083-09.pdf, 21 April 2020.

45. European Union, Court of Justice of the European Union. (2000). *Opinion of Mr Advocate General Alber in The Queen v Minister of Agriculture, Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61998CC0369, 4 March 2020.

46. European Union, Court of Justice of the European Union. (2007). *Opinion of Mr Advocate General Kokott in the Promusicae* case. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A62006CC0275, 5 March 2020.

47. European Union, Court of Justice of the European Union. (2013). *Opinion of Mr Advocate General Wathelet in European Commission v Germany*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CC0288, 6 March 2020.

48. European Union, Court of Justice of the European Union. (2017). *Opinion 1/15 of the Court (Grand Chamber)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62015CV0001(01)&from=EN, 1 May 2020.

49. European Union, Court of Justice of the European Union. (2020). *Advocate General's Opinions in Case C-623/17 Privacy International, Joined Cases C-511/18 La Quadrature du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others.* Retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-01/cp200004en.pdf?fbclid=IwAR1AagKfvXXxUvRmaNL1yIy-kQwt8GLQX-lNoOBs7O83n0M3VqW8yuDV8S8, 23 March 2020.

50. European Union, European Commission. (2008). *Commission Staff Working Document: Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Report on the evaluation and future development of the FRONTEX Agency: Impact assessment*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52008SC0148, 31 January 2020.

51. European Union, European Commission. (2008). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Preparing the Next Steps in Border Management in the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52008DC0069&from=ga, 31 January 2020.

52. European Union, European Commission. (2010). *Communication from the Commission on Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0573:FIN:en:PDF, 30 February 2020.

53. European Union, European Commission. (2013). *Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EC) No 562/2006 as regards the use of the Entry/Exit System (EES) and the Registered Traveller Programme (RTP)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0096&from=EN, 11 February 2020.

54. European Union, European Commission. (2016). *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System*. Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:4e2ac515-fca4-11e5-b713-01aa75ed71a1.0014.02/DOC_1&format=PDF, 31 January 2020.

55. European Union, European Commission. (2016). *Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011*. Retrieved from https://eur-lex.europa.eu/resource.html?uri=cellar:19cfa4b9-fca5-11e5-b713-01aa75ed71a1.0020.02/DOC_1&format=PDF, 31 January 2020.

56. European Union, European Union Agency for Fundamental Rights. (2015). *Fundamental Rights Implication on the Obligation to Provide Fingerprints for Eurodac.* Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-fingerprinting-focus-paper_en.pdf, 3 March 2020.

57. European Union, European Union Agency for Fundamental Rights. (2018). *Under watchful eyes: Biometrics, EU IT systems and Fundamental Rights*. Retrieved from https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf, 4 March 2020.

58. European Union, European Parliament. (1999). *Conclusions of the European Council in Cologne*. (Annex IV). Retrieved from https://www.europarl.europa.eu/summits/kol2_en.htm#an4, 20 February 2020.

59. M. Oostveen., K. Irion. (2016). *The Golden Age of Personal Data: How to Regulate an Enabling Fundamental Right?*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885701, 3 March 2020.

Appendix 1. Non-exclusive licence

Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I, Essi Lumiaho;

1. Give Tallinn University of Technology a permission (non-exclusive licence) to use, free of charge, my creation

The Implications of Advancements in Smart Borders Package Biometric Data Collection and Storage Technology on the Rights of the Individual in the Context of the EU Charter of Fundamental Rights,

supervised by Jenna Uusitalo,

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive licence, no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive licence is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*