Bachelor Thesis

"The search for autonomy" – The UK's quest for data protection autonomy, as illustrated in the case of EU-UK PNR data transfers

29. June 2022

Thesis Supervisor: Dr. Claudio Matera

Second Supervisor: Dr. Guus Meershoek

Version: 14

Word count: 12000

Patrick Ryan Berndt

Public Governance across Borders (PGaB)

Faculty of Behavioural, Management and Social Sciences (BMS)

University of Twente, Enschede

Westfälische Wilhelms-Universität, Münster

Abstract

With the United Kingdom's formal exit from the European Union and its new status as a "third-country" come a host of diverse and intricate legal issues which will challenge policy-makers for years to come. One of the most divisive of these challenges is the protection and transfer of personal data between the EU and the UK currently regulated in the "Trade and Cooperation Agreement". With the UK determined to re-claim its (data) sovereignty through Brexit and the EU focussed on utilizing its normative power to "export" its high fundamental rights standards on privacy and personal data protection to third countries, serious "data de-harmonization" is brewing. This thesis analyses the UK's possibilities to develop an autonomous regime of data protection, illustrated through the specific example of Passenger Name Record Data. Accordingly, the thesis evaluates the EU's internal and external dimensions of PNR data, before discussing the EU-UK PNR data transfer under the TCA and the UK's plans to diverge from these provisions so as to create its own autonomous (PNR) data regime. As a thesis founded upon public governance studies in a legal context, it employs a qualitative research design based on hermeneutics, focussing specifically on descriptive, evaluative and interpretive characteristics.

Table of contents

List of abbreviations

List of abbreviations

AFSJ	Area of Freedom, Security and Justice
AG	Advocate General
AI	Artificial Intelligence
CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
DPA	Data Protection Act
ECHR	European Convention on Human Rights
ECSC	European Coal and Steel Community
EDPS	European Data Protection Supervisor
EEAS	European External Action Service
EU	European Union
GDPR	General Data Protection Regulation
LED	Law Enforcement Directive
NPO	Non-profit Organisation
PIU	Passenger Information Unit
PNR	Passenger Name Record
TCA	EU-UK Trade and Cooperation Agreement
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TIGRR	Taskforce on Innovation, Growth and Regulatory Reform
UDHR	Universal Declaration of Human Rights
UK	United Kingdom
UN	United Nations
US	United States

1. Introduction

1.1. Thesis overview

Of all the challenges brought about by the United Kingdom's (UK) 2016 Brexit referendum and subsequent departure from the European Union (EU), those concerning data protection and data transfers might be among the thorniest. The EU is – in the area of data protection as much as in most other policy areas – insistent upon ensuring the highest set of standards in the world (European Commission, 2020a, pp. 28, 33), a fact that was recently emphasised with considerable force through the adoption of Regulation 2016/679, more commonly known as the "General Data Protection Regulation" (GDPR). This legislative milestone is the Union's foremost tool to ensure its citizens personal data are protected, thereby guaranteeing Art. 8 of the Charter of Fundamental Rights of the European Union (CFREU) on the protection of personal data (European Union, 2012a, Art. 8).

One EU data mechanism which has repeatedly encroached upon – or, as some scholars argue, outrightly breached (Thönnes, 2022a) – the CFREU is the collection, transfer, and use of so-called "Passenger Name Record" (PNR) data. EU Directive 2016/681 – adopted alongside the aforementioned GDPR – from hereon referred to as the "PNR Directive", regulates the collection, use, retention, and transfer of air passenger's personal information. These data are collected by air carriers and include information "such as the name of the passenger, travel dates, itineraries, seats, baggage, contact details and means of payment" (European Council, 2021). Since these data are obtained from *every* air passenger, this mechanism is one of mass data collection and thus stands in contention with the right to personal data protection. A justification for this infringement is offered in Art. 1 of the PNR Directive, which limits the use of PNR data to "the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime [...]." (European Parliament/Council, 2016a).

With the UK's exit from the EU on the 31.01.2020 and the subsequent expiry of the "transitional period" – during which EU law continued to apply in the UK – on the 31.12.2020, the UK became a "third country" in regards to the EU, with far-reaching implications for all policy fields, including data. Crucially, the UK in 2018 amended its national law – the "Data Protection Act" (DPA) – to include all EU GDPR provisions, thereby adopting the same regulations and standards on data protection (UK Government, n.d.). Concerning PNR data, Title III of Part Three of the "EU-UK Trade and Cooperation Agreement" (TCA) regulates the EU-UK exchange of such data. Regarding data transfers between the EU and a third country, a crucial aspect has been the adoption of so-called "adequacy decisions" by the European Commission. On the legal basis of Art. 45 GDPR the Commission can adopt such a decision, thereby declaring that a third country possesses "adequate" data protection standards to allow for data transfers between it and the Union (European Parliament/Council, 2016b, Art. 45). In the case of the UK, such adequacy decisions were adopted on the 28. June 2021 (European Commission, 2021).

The above description demonstrates that the EU holds its Member-States and third countries to high data protection standards. It is therefore interesting to analyse how the UK – having expressed its wish for greater freedom through the Brexit referendum – could develop an autonomous regime of data protection in the context of the regulations outlined above. Furthermore, the potential development of such an autonomous data protection regime could be symbolic for the overall "success" of Brexit and the fulfillment of the "Vote Leave"-campaigns mantra of "taking back control" (Haughton, 2021). It is this "attainment of autonomy" which makes the example of PNR data transfers so interesting to analyse. The current relevance of this topic is enhanced due to the fact that the Court of Justice of the European Union (CJEU) has begun cracking down on inadequate third-country PNR

agreements, as demonstrated by its precedent-setting Opinion 1/15 concerning the draft EU-Canada agreement.

Encapsulating the issue outlined above, this thesis paper aims at answering the following main research question: *To what extent does the post-Brexit "Trade and Cooperation Agreement" (TCA) allow the UK to develop an autonomous regime of data protection?* To guide the analysis, several sub-questions have been formulated, which will be answered in turn: (1) What are the principal regulatory regimes for data protection and PNR in the EU?; (2) To what extent is the EU allowed to share PNR data with third countries?; (3) To what extent could the UK – under the provisions of the TCA – diverge from EU standards and principles on data protection and PNR data transfers?

1.2. Theory

Identifying a theoretical foundation suitable to the analysis of current EU-UK data transfers as well as to the ways in which this process could change in the future is no straightforward task. Never in the EU's history has a Member-State left the Union, making Brexit "[...] a unique case of disintegration [...]" (Gstöhl/Phinnemore, 2021, p. 99). The unprecedented nature of Brexit means that scholars are "tapping in the dark" when trying to evaluate Brexit from a theoretical perspective, since the political/legal situation is ever-evolving. Nevertheless, the following sub-sections outline two theoretical approaches which – when applied to the issue of EU-UK data transfers, *inter alia* PNR data – can be used to evaluate the UK's possibilities of creating an autonomous data regime.

1.2.1. Normative Power Europe

When discussing the concept of the EU as a normative power, one cannot avoid Ian Manners' influential article "Normative Power Europe: A Contradiction in Terms?", published in the Journal of Common Market Studies in 2002. Through the historical context from which the European Coal and Steel Community (ECSC) was born in 1951, and increasingly since the codification of the "Treaty on European Union" (TEU) in 2007, the EU has placed certain norms at the centre of its political activity. Manners defines these norms as "the principles of democracy, rule of law, social justice and respect for human rights [...]" (Manners, 2002, p. 241). The EU's focus on upholding these principles both within its own borders as well as in regards to third countries is – according to Manners – the way in which the EU materialised itself internationally as a distinctively "different" actor (2002, pp. 240-242). With the EU being such a normative power, Manners states that this has a profound impact on the way the EU engages in international politics, declaring that the EU is inherently "predispose[d] [...] to act in a normative way in world politics." (2002, p. 252).

Connecting this theoretical concept to the issue underlying the thesis, it can be expected of the EU to conclude third-country agreements only with countries willing to accept the above norms. Pertaining to data, the norm which is predominantly touched upon is the safeguarding of certain human rights. Firstly, the right to privacy is a fundamental human right which has been codified in various treaties and declarations: the United Nations (UN) Universal Declaration of Human Rights (UDHR) Art. 12 states that "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.*" (United Nations, 1948). In similar fashion, the European Convention on Human Rights (ECHR) states that *"Everyone has the right to respect for his private and family life, his home and his correspondence."* (European Court of Human Rights/Council of Europe, 2021, Art. 8(1)). Finally, the CFREU reiterates this basic human right:

"*Everyone has the right to respect for his or her private and family life, home and communications."* (European Union, 2012a, Art. 7). The other relevant human right – the right to personal data protection – gained relevance recently owing to the advancements of the digital age and the resulting increase in data. As such, the UN UDHR, codified in 1948, does not contain a provision on the protection of personal data. The EU however has codified this fundamental human right: Art. 16 of the Treaty on the Functioning of the European Union (TFEU) as well as Art. 8 of the CFREU both state that "*Everyone has the right to the protection of personal data concerning him or her.* (European Union, 2012a, Art. 8(1)).

The EU as a normative power tries to "export" these human rights through its external relations and therefore aims to adopt international data agreements only with countries which themselves uphold these rights. Concerning EU-UK PNR data transfers, Art. 524 TCA bases all cooperation codified in Part Three of the TCA – *inter alia* the transfer of PNR data – on the mutually acknowledged "*[...] respect for democracy, the rule of law and the protection of fundamental rights and freedoms of individuals, including as set out in the Universal Declaration of Human Rights and in the European Convention on Human Rights [...]"* (European Union, 2021).

1.2.2. UK sovereignty

A theoretical concept standing in contention to that of "normative power Europe" is the concept of UK sovereignty/autonomy, which the "Leave campaign" promised Brexit would deliver. There are multiple aspects to consider here, including the Leave campaigns role in the outcome of the referendum and the conceptualization of sovereignty in the UK, which is based on the unique idea of "parliamentary sovereignty".

The starting point therefore is the "traditional" definition of sovereignty: as a concept created during the Enlightenment period, sovereignty refers "[...] to the ability of a state to make decisions about events within its borders without external inference." (Verovšek, 2020). Through the processes of globalization, this traditional understanding of state sovereignty has been all but eliminated from most industrialised nations, and intergovernmental/supranational organisations – such as the EU – were implicitly founded upon the idea of nation states "giving up" parts of their sovereignty for the mutual (economic) benefit of all. Taking this reality into account, Verovšek notes that international economic agreements and institutions "[...] such as the EU's single market do not reflect a loss but a pooling of sovereignty [...]." (Verovšek, 2020). Dr. Nicholas Westcott, formerly the UK's main diplomat in the "European External Action Service" (EEAS), advances this conceptualization, stating that "[...] real sovereignty means having a seat at the table, a voice in the debate and a vote on the outcome." (Westcott, 2020). This statement summarizes the powers the UK possessed as an EU Member-State and links back to Verovšek's claim that EU-membership does not mean an inherent loss of sovereignty.

To understand why the UK's electorate therefore decided to reject the "seat at the table" and voted to leave the EU, one must understand the role which the primary campaigning organisation backing a "leave" vote in the referendum played, namely the "Vote Leave" campaign, founded in October of 2015 and backed by prominent political figures across the party-political spectrum (BBC, 2015). Most notably, then-mayor of London and current Prime Minister of the UK, Boris Johnson, was publicly outspoken about his support for the campaign and became a key "Vote Leave" spokesperson (BBC, 2016). The campaigns central message was described by BBC as being "[...] about sovereignty, with 'take control' the main slogan." (BBC, 2015). This resonated strongly with the electorate,

with Bellamy even declaring that "the Brexit referendum was won on the slogan 'taking back control'" (Bellamy, 2020). Undoubtedly, the "Vote Leave" campaign was highly influential, not only through shaping the minds of many voters, but also by advancing the particular understanding of the concept of sovereignty prevalent in the UK today.

"Taking back control" implies understanding sovereignty traditionally, with a focus on the "[...] control over our borders, our trade and our money [...]." (Westcott, 2020). The reason why the UK retains this understanding relates to the principle of "parliamentary sovereignty", the functional core of the UK's uncodified constitution, which "[...] makes Parliament the supreme legal authority in the UK, which can create or end any law." (UK Parliament, n.d.). This position of absolute power is unique amongst today's modern democracies, as most countries possess codified constitutions which limit their parliament's power, (e.g. Germany's "Grundgesetz"). The principle of parliamentary sovereignty and especially its limitation through the UK's accession to the EU in 1973 was the driving force behind the "special EU-UK relationship" during the UK's membership and explains the many concessions and special rules the UK benefitted from, such as Thatcher's infamous "UK rebate". The UK's displeasure with the EU's ability to pass legally binding acts and therefore to "overrule" parliamentary sovereignty created ongoing friction for years before the eventual referendum, with "Tagesschau" declaring in 2013 that the UK "always has one foot outside the door" of EU membership (Tagesschau, 2013). The significance of parliamentary sovereignty for the UK is such that it is expressly stated in the "European Union (Withdrawal Agreement) Act 2020": as codified in section 38(1), "It is recognised that the Parliament of the United Kingdom is sovereign." (UK Government, 2020, section 38(1)).

This theoretical section has outlined two theories/concepts that can be used to analyse the future of EU-UK (PNR) data transfers: the concept of "normative power Europe" stands contrasted to the *de jure* sovereignty the UK has (re)gained through Brexit. Whether the UK also benefits from this sovereignty *de facto* and whether this allows it to create an autonomous data regime whilst also adhering to the strong normative EU requirements on human rights is analysed in this thesis.

1.3. Methodology

This thesis aims at answering the central question, "*To what extent does the post-Brexit "Trade and Cooperation Agreement" (TCA) allow the UK to develop an autonomous regime of data protection?"*. To answer this question, the thesis adopts a qualitative research design based on textual analysis. The method of textual analysis can be traced back to the research paradigm of constructivism and was influenced by people such as the German sociologist Max Weber (Given, 2008, p. 116). The focus of constructivist research is an interpretive/hermeneutical approach to *understanding*, which represents a shift from the natural-science based notion of *explaining*, and is described as being "*[...] more appropriate for investigating phenomena in the human sciences."* (Given, 2008, p. 116). This focus on understanding stems from the ontological assumptions of the constructivist paradigm that reality and knowledge are social constructs and therefore subjective. Since constructivists do not believe in an objective/external reality, no "ultimate" truth can be discovered. Consequentially, to achieve constructivist *understanding*, the subjective context in which an observed phenomenon develops must be considered. The methodology of hermeneutics/interpretive research has long been used to understand legal and biblical texts, since the approach is able to facilitate *understanding* of such texts by providing the relevant historical, social, political and/or cultural context (Given, 2008, p. 386).

This thesis adopts a hermeneutical/interpretive research approach as its guiding methodology to answer the main research question along with the sub-questions, which themselves contain a variety of interpretive research characteristics: the first sub-question, *"What are the principal regulatory regimes for data protection and PNR in the EU?",* adopts a descriptive nature and creates a knowledge base concerning the regulatory framework of data protection and PNR in the EU. This section draws textual data from primary and secondary EU law, such as the TFEU and CFREU (primary) and GDPR and PNR Directive (secondary). The second sub-question, *"To what extent is the EU allowed to share PNR data with third countries?"* combines descriptive and evaluate aspects, focussing on the conditions under which the EU shares PNR data with third countries as codified in legal texts (PNR Directive) and case law (Opinion 1/15). This section also uses existing research from published scholars in the form of scientific articles and opinion pieces. Finally, the third sub-question, *"To what extent could the UK – under the provisions of the TCA – diverge from EU standards and principles on data protection and PNR data transfers?"* adopts explanatory, evaluative and interpretive characteristics, directing the focus to the EU-UK PNR data transfers and drawing heavily from the relevant provisions of the TCA, as well as from the knowledge generated throughout the previous sub-questions, to evaluate the UK's possibilities of diverging from the current TCA provisions on (PNR) data.

The thesis thus utilises a variety of research characteristics situated within the methodological orientation of hermeneutical/interpretive research. Specifically the descriptive and evaluative aspects are situated firmly within the interpretive framework: *"In interpretive research [...] The emphasis is on sensemaking, description, and detail."* and *"Evaluation research is applied in that the aim is to produce knowledge that will contribute to greater understanding [...]."* (Given, 2008, pp. 465, 303). Therefore, the methodology of hermeneutics is the logical choice for this thesis.

2. The EU's regulatory framework on data protection and PNR data

The following section focusses on the regulatory framework regarding data protection and PNR data within the EU, therefore constituting the "internal dimension" of the thesis. As such, the section aims at answering the sub-question: *What are the principal regulatory regimes for data protection and PNR in the EU?* Answering this sub-question first – before introducing the "external dimension" of third-country PNR data transfers in section 3 – is important, since the legislative provisions regulating personal data protection and PNR *within the EU* significantly influence the nature of these same processes *outside the EU.* This section therefore builds a knowledge base required for the comprehension of the thesis' subsequent sections.

When addressing the EU's internal framework on data protection and PNR data, the starting point must always be the comprehensive "data protection reform package", which comprised three pieces of EU legislation adopted simultaneously in April of 2016. More concretely, these are the previously mentioned GDPR (Regulation 2016/679) and PNR Directive (Directive 2016/681), as well as the so-called "Law Enforcement Directive" (LED) (Directive 2016/680), which regulates police and judicial procedures concerning data protection in the EU. The following sub-sections will address each of these legislative acts in turn.

2.1. The "General Data Protection Regulation" (GDPR)

As mentioned above, the GDPR is a landmark legislative act and constitutes the most comprehensive set of regulations on the protection of personal data and data privacy for EU citizens. Adopted in April of 2016, the GDPR is directly binding for all Member-States and entered into force on the 25. May 2018, thereby repealing the EU's previous framework on personal data protection, the "Data Protection Directive" (Directive 95/46/EC). Focussed on strengthening the data rights of individuals, the GDPR encapsulates many key provisions which set the benchmark for the processing of personal data and thus acts as the EU's foremost regulatory tool to guarantee the fundamental right of personal data protection (Art. 8 CFREU). This "guarantee" is most explicit in Art. 5 GDPR, which codifies seven "Principles relating to processing of personal data" (European Parliament/Council, 2016b), which also have a profound effect on how PNR data is handled.

Art. 5(1a) codifies the importance of "lawfulness, fairness and transparency" when handling personal data (European Parliament/Council, 2016b). This provision limits the processing of personal data to cases in which it is *lawful* to do so, which includes reasons such as pursuing a significant public interest (e.g. preventing terrorism/serious crime), but also enables service providers to process personal data if the user has consented. Furthermore, using personal data *fairly* means being *transparent* about the reasons and ways data is processed, thereby giving individuals the possibility to see which data is being collected and for which purpose. Further principles relevant in regards to PNR are those of "purpose limitation and data minimisation" (Art. 5 (1b,c)). As per GPDR definition, data may only be "collected for specified, explicit and legitimate purposes [...]." (European Parliament/Council, 2016b). EU regulatory acts such as the PNR Directive define their purpose of data collection, and – pursuant to this provision – cannot extent the collection beyond that purpose. Furthermore, data minimisation ensures that only the smallest amount of data needed to achieve this purpose is collected, thereby restricting unnecessary/excessive data collection. Summarizing, the principles detailed above create a bridge between the GDPR and the fundamental human rights codified in Art. 8 CFREU, whilst also respecting the principle of proportionality (Art. 52 CFREU). Relating this to the theory of "normative power Europe", it is apparent how the EU aims to solidify its commitment to human rights by enshrining them in the GDPR.

2.2. The "Law Enforcement Directive" (LED)

Connecting personal data protection to EU law enforcement, security, and counter-terrorism leads to a discussion of the LED, which was adopted in 2016 and – as a Directive – required transposition into Member-States' national law by the 6. May 2018. This Directive constitutes one of the two supplementary acts to the GDPR, operating alongside it and regulating personal data protection in the law enforcement environment. As such, Art. 1 LED states that it "*lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.* (European Parliament/Council, 2016c). The PNR Directive – which possesses a strikingly similar purpose – is therefore *lex specialis* to the LED, as the EU saw the necessity for a separate act regulating matters concerning PNR data.

Linking the need to process data for law enforcement purposes and the requirement to protect individuals personal data, the LED in Art. 4 essentially adopts the same principles of data processing as codified in the GDPR, with the exception of the *transparency* requirement, which is difficult to implement in a security/law enforcement context operating predominantly with classified data

(European Parliament/Council, 2016c, Art. 4). Generally, personal data protection rights in the LED are upheld to the standards set by the GDPR, "however, there is greater scope for these rights to be limited than under the GDPR." (Citizens Information, 2021), which can be attributed to the purpose of the LED to prevent the most serious crimes.

2.3. The "Passenger Name Record Directive" (PNR)

Finally, the third legislative act of the EU's *internal* framework on personal data protection – and the most relevant for this thesis– is the "PNR Directive", which was adopted in April 2016 and was to be transposed into national law by Member-States by the 25. May 2018, the same day the GDPR entered into force. Although the EU had been collecting, using and transferring PNR data before the Directive was adopted (see section 3.1.), it was only with this Directive that the EU gave itself a comprehensive regulatory framework on PNR data which also respected the standards and principles codified by the GDPR. Since this section is concerned only with the *internal* EU dimension, provisions in the Directive regulating the *external* dimension (Art. 11, 21) will not be addressed here, but rather discussed in detail below (see section 3.2.)

2.3.1. Provisions and European Commission review of the PNR Directive

The PNR Directive primarily provides for the collection of PNR data received from airlines operating "extra-EU flights" into or out of an EU Member-State (Art. 1), but may also be applied to data collection from "intra-EU flights" between EU Member-States (Art. 2), a provision which as of 2020 has been applied by all but one Member-State (European Commission, 2020b, p. 10). The purpose of PNR data collection and processing is limited to "preventing, detecting, investigating and prosecuting terrorist offences and serious crime [...]" (Art. 1(2)). A noteworthy aspect is the dual-purpose of the Directive to combat crime both *ex ante* as well as *ex post*. Especially the purpose of *preventing* terrorist offences or serious criminal acts (ex ante) is an argument in favour of the "generalized" data collection of *every* air passenger occurring under the Directive.

After initially regulating scope and purpose, the Directive next addresses the "Responsibilities of the Member States" (Chapter II), which include the most important provisions on PNR data, many of which relate back to the standards and principles of the GDPR. Art. 4 codifies the obligation of each Member-State to create an institution called a "Passenger Information Unit" (PIU). Airlines collecting PNR data are required (Art. 8(1)) to transfer those data to the PIU's, which are responsible for "storing and processing" the data. Furthermore, the PIU's are charged with exchanging PNR data with other Member-States' PIU's and with Europol, as well as forwarding PNR data to a Member-States' so-called "competent authorities" (Art. 7) in cases where PNR data is required to fulfill the Directive's purpose. Concerning the processing of PNR data by PIU's, specifically for which purposes this may occur is regulated in Art. 6, whereas Art. 12 regulates "data retention and depersonalisation", requiring each PIU to store PNR data in their database for five years before permanently deleting them, as well as ensuring data depersonalisation after six months. Furthermore, Art. 13 links the Directive to the GDPR by addressing the "protection of personal data", giving individuals data protection rights such as the "right of access, rectification, erasure and restriction [...]". The Directive also prohibits the processing of sensitive personal data through Art. 13(4), placing additional safeguards on PNR data which might "[reveal] a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.". These safeguards relate back to the provisions of the GDPR and the CFREU's fundamental human rights.

The European Commission – acting upon the requirement of Art. 19(1) of the Directive – presented a review report to the European Parliament and the Council on the 24. July 2020, in which it evaluated the first two years of the Directive being in force. The Commission initially reviewed the extent to which Member-States had been able to transpose the Directive on time and in adherence to the required provisions, declaring that at the time of review all but two Member-States had fully transposed the Directive (the exceptions being Slovenia and Spain) and that "a vast majority" of Member-States had created "fully operational" PIU's (European Commission, 2020b, p. 5). More relevant however is the Commission's evaluation of the Member-States' adherence to data protection standards, during which it found "an overall compliance with the data protection requirements of the PNR Directive [...]" (European Commission, 2020b, p. 5). The Commission subsequently addressed many of the most critical or controversial aspects of the Directive, such as the "generalized/broad" collection of PNR data as well as the need to retain PNR data for five years, coming to the conclusion that these provisions are proportional (European Commission, 2020b, pp. 6-7).

2.3.2. Case C-817/19

Whilst the Commission report paints a favourable picture of the PNR Directive and its compatibility with the EU's human rights framework concerning personal data protection, it remains far from unchallenged. On the 31. October 2019, the Belgian constitutional court requested a preliminary ruling from the CJEU on the compatibility of the Directive with EU primary law. The case – officially numbered C-817/19 – was brought before the Belgian constitutional court by "the non-profit organisation (NPO) '*Ligue des droits humains'* [who] opposed the broad definitions of PNR data and 'passengers' [...]." (Wahl, 2022). Other aspects of the Directive – including those reviewed positively by the Commission, such as the five-year retention period – were also criticized by the NPO.

On the 27. January 2022, the CJEU's Advocate General (AG) Pitruzzella released his (non-binding) opinion on the case. In it, he criticised certain aspects of the Directive as being incompatible with the human rights framework of Art. 7, 8 CFREU, such as the use of the category "General remarks" in point 12 of Annex I of the Directive as a category of PNR data to be collected by airlines, stating that this definition "did not satisfy the conditions of clarity and precision [...]" required by the CFREU (CJEU, 2022a, p. 2). Such a broad definition could lead to the collection of sensitive personal data, which the Directive prohibits (European Parliament/Council, 2016a, (37)). Furthermore, the AG found the retention period of five years for *all* PNR data (Art. 12(1)) to exceed "what is strictly necessary" and stated that five-year retention is "[...] justified only where there is a serious threat to the security of the Member States [...]." (CJEU, 2022a, p. 3). However, a more notable consequence of this opinion was the fact that whilst the generalized retention of all PNR data was declared as incompatible with the CFREU, the "generalized and undifferentiated nature of the transfer of PNR data [...] is compatible with Articles 7 and 8 of the Charter [...]." (CJEU, 2022a, p. 2). "Generalized and undifferentiated" here means the collection and transfer of PNR data from *all* air passengers, not only those previously suspected of involvement in serious criminal or terrorist activities. This opinion on the fundamental compatibility of the Directive with the human rights framework of the CFREU "[...] is a disappointment to civil society organisations hoping for the invalidation of the PNR Directive [...]." (EDRi, 2022). Many have criticized the "indiscriminate" collection of personal data under the Directive, such as scholar Christian Thönnes, who reacted to the AG's opinion by declaring it "a cautious green light for technology-driven mass surveillance" and subsequently argued for the Directive's invalidation (Thönnes, 2022a), as well as human rights organisation EDRi, which stated that "the PNR Directive amounts to mass surveillance similar to general and indiscriminate data retention of telecommunications metadata." (EDRi, 2022). The CJEU on the 21. June 2022 ruled in the

matter of C-817/19 and – by performing multiple "proportionality tests" to determine whether the Directive's mechanisms are limited to "what is strictly necessary" – agreed with the AG's above opinion, stating that PNR data as described in Annex I must be limited to "clearly identifiable and circumscribed information" and declaring that the retention of *all* air passengers PNR data after the initial six-month retention period goes "beyond what is strictly necessary." (CJEU, 2022b, pp. 2, 4). The CJEU also extended its scrutiny of the Directive beyond the points addressed by the AG, prohibiting AI-based automated processing of PNR data, as well as declaring that the application of the Directive to intra-EU flights must be limited to cases in which a Member-State is facing a "genuine and present or foreseeable" terrorist threat (2022b, p. 2).

2.4. Conclusion on the EU's regulatory framework on data protection and PNR data

The above section aimed at answering the sub-question: "*What are the principal regulatory regimes for data protection and PNR in the EU?".* In this regard, the main regimes constituting the EU's *internal* framework on data protection and PNR data are the GDPR, LED, and PNR Directive discussed above. These regulatory acts enshrine many fundamental principles, such as proportionality (data minimisation), transparency, adequacy, purpose limitation and time-sensitive data retention, along with strong individual data rights, including the rights of access, erasure and rectification. Overall, this internal framework possesses a strong connection to the fundamental rights to privacy and personal data protection of the CFREU (Art. 7, 8, 52), although as discussed (C-817/19) it can be argued that these rights are not protected strongly enough against interference, especially from the PNR Directive.

3. The EU's third country agreements on PNR data

After having discussed the *internal dimension* of data protection and PNR, this section turns its attention to the *external dimension* regarding PNR data transfers between the EU and third countries, so-called "third-country PNR agreements". The section opens with an overview of the historical developments of EU external PNR agreements, before discussing the legislation on present-day third-country PNR agreements. Concretely, this includes the provisions of the PNR Directive concerning third-country data exchanges (Art. 11, 21), the significance of the GDPR's "adequacy decisions", as well as an analysis of the most prominent CJEU ruling regarding PNR data, Opinion 1/15 on the draft EU-Canada agreement. The discussion of these aspects allows this section to provide an answer to the second sub-question: *To what extent is the EU allowed to share PNR data with third countries?*

3.1. The historical development of third-country PNR agreements

The history of PNR data being collected, used and exchanged for the purpose of preventing and combating serious crime and terrorism does not begin with the EU's PNR Directive, but rather can be traced back to the 9/11 terrorist attacks in the United States (US). In the wake of these attacks, the western world focussed on making air travel safer and less vulnerable to terrorist incursions. The US, wanting to demonstrate its nation's strength and resilience, led the way and quickly identified PNR as "[...] invaluable tools for investigating and thwarting terrorist attacks." (Hobbing, 2008, p. 6). Seeking to strengthen its borders against future terrorist threats via air travel, the US efforts culminated in the adoption of the "Aviation and Transportation Security Act" on the 19. November 2001,

which required every US-bound international flight to submit PNR data to US Customs authorities (Hobbing, 2008, p. 7). This created a legislative "nightmare" for international airlines, as they were required by US law to submit PNR data to the relevant authorities, but in doing so " [...] would violate EU data protection provisions" and therefore automatically break EU law (Hobbing, 2008, p. 7). It is as a result of this legislative "de-harmonization" that the EU and US opened negotiations on a bilateral agreement, ultimately leading to the adoption of the first EU-US PNR agreement in 2004.

Whilst the EU-US PNR saga has been fraught with challenges (the 2004 agreement barely survived two years before being invalidated by the CJEU in 2006 and the current agreement adopted in 2012 is the subject of constant criticism), it is nevertheless relevant to reflect upon how the EU came to enter into its first third-country PNR agreement, as the situation exemplifies how the EU occasionally does not manage to exert its "normative power". Specifically in the above case, the lack of an *internal* EU framework on PNR led to the Union becoming a "norm-taker", internalizing many US border security norms (Argomaniz, 2009, p. 119). Because the EU also entered into other third-country PNR agreements (Canada in 2006, Australia in 2008) and this increased usage of PNR data needed to be met with equally strong standards on personal data protection, the Commission in 2010 published a communication which revised its "global approach to the transfer of PNR data to third countries" (European Commission, 2010, p. 2). The Communication focussed on standardizing the provisions regulating third-country PNR data transfers throughout all agreements, as well as ensuring high levels of data protection pursuant to the EU's fundamental human rights framework. This new approach resulted in the re-formulating of all existing third-country PNR agreements, with the "second-generation" US and Australia agreements being adopted in 2012, whilst the proposed EU-Canada agreement was not ratified by the European Parliament and ultimately became the subject of the CJEU's Opinion 1/15.

3.2. The legislative provisions regulating the EU's third-country PNR agreements

The previously omitted provisions of the PNR Directive concerning the *external* dimension are now addressed in light of their effect on the means in which the EU shares PNR data with third countries. Firstly, the Directive does not exclusively regulate the exchange of PNR data between a third country and the *entire* EU, but also provides for data exchanges between *individual* Member-States and third countries. Art. 21(1) states that "Member States may continue to apply bilateral or multilateral agreements or arrangements between themselves [...]" (European Parliament/Council, 2016a), as long as such agreements are not incompatible with the provisions of the Directive. Furthermore, Art. 21(3) notes that the Directive does not encroach upon or invalidate existing agreements which Member-States or the Union have adopted with third countries. Owing to the EU's and Member-States' shared competence in the "Area of Freedom, Security and Justice" (AFSJ), the Directive cannot "override" such existing agreements (European Union, 2012b, Art. 4(2j)).

Art. 11 of the Directive regulates when and how an EU Member-State may transfer PNR data to a third country, underlining the importance of transferring data only for the specific purpose of the Directive, as well as the need to adhere to the same processes as regulated in the Directive (e.g. the creation of a PIU). Art. 11(1a) links the third-country transfer of PNR data to the "conditions laid down in Article 13 of Framework Decision 2008/977/JHA", a piece of EU legislation which is no longer in force since being repealed by the LED in 2016. However, the conditions referred to in Art.11(1a) continue to exist in the LED's "Chapter V" on the "Transfer of personal data to third countries or international organisations" (European Parliament/Council, 2016c). Another important provision is Art. 11(1c), which permits so-called "onward transfer" of PNR data that a third country

has received from the EU to another third country, albeit "only where it is strictly necessary". This provision creates the possibility of EU PNR data being forwarded beyond the limits of the initial third-country agreement and therefore poses a threat to the fundamental rights of privacy and personal data protection.

The other legislative tool the EU possesses in regards to third-country transfers of PNR data – the "adequacy decision" – can be found in Art. 45 GDPR. As mentioned in this thesis' introduction, an adequacy decision is a decision which declares a third country to possess an "adequate" (to be understood as "sufficient") level of data protection. For third countries possessing an adequacy decision, personal data transfers with the EU (including PNR data transfers) "[...] shall not require any specific authorisation." (European Parliament/Council, 2016b, Art. 45(1)), enabling personal data to flow freely. Whilst the further provisions of Art. 45 describe aspects such as the required periodic review of the third countries' level of data protection (at least once every four years), the most important aspect of Art. 45 is its connection to the EU's "[...] human rights and fundamental freedoms [...]." (Art. 45(2a)). Just as section 2.1. of this thesis found that the EU through the principles codified in the GDPR evokes *normative power* upon its Member-States to uphold the fundamental rights of privacy and personal data protection, a review of Art. 45 demonstrates how the EU also tries to *export* these norms to third countries, thereby relating back to the theory of "normative power Europe".

3.3. The CJEU's Opinion 1/15

On the 30. January 2015 the European Parliament requested an opinion from the CJEU on the legal basis of Art. 218(11), which permits the Parliament to enquire "[...] as to whether an agreement envisaged is compatible with the Treaties." (European Union, 2012b). In its request, the Parliament focussed on two aspects: first, whether the proposed agreement was compatible with EU Treaty provisions regulating privacy and personal data protection (Art. 16 TFEU, Art. 7, 8 CFREU) and the principle of proportionality (Art. 52(1) CFREU), and secondly, whether Art. 82(1) and 87(2a) TFEU constituted the correct legal basis for the proposed agreement. The ruling, issued by the CJEU on the 26. July 2017 and numbered "Opinion 1/15", constitutes one of the most significant CJEU rulings on data protection and PNR and has had widespread effect on both the *internal* and *external* dimension of EU data transfers, including on the TCA provisions regulating the EU-UK PNR data transfer. Most notably, Opinion 1/15 set precedence by way of being "[...] the Court's first ruling on the compatibility of a draft international agreement with the EU Charter of Fundamental Rights [...]." (Kuner, 2017).

3.3.1. The correct legal base(s)

Concerning the question of the correct legal base, the Court initially expressed that in cases where an agreement pursues more than one purpose and a "predominant purpose" cannot be determined, such an agreement must "[...] be founded on the various corresponding legal bases [...]. (CJEU, 2017, para. 77). The Court then analysed the purpose(s) of the envisaged EU-Canada agreement, coming to the conclusion that not only does the agreement pursue multiple purposes ("ensuring public security" (para. 82); ensuring the protection of personal data (para. 83-84)), but that these purposes are also "inextricably linked" (para. 94). The CJEU therefore ruled that third-country PNR agreements must always be founded on *at least* two legal bases, so as to cover both these purposes. The Court determined Art. 16(2) and Art. 87(2a) TFEU as the correct legal bases for the proposed agreement (para. 118), since Art. 87(2) – which regulates police cooperation for the "prevention, detection and

investigation of criminal offences" (European Union, 2012b) – relates to the purpose of "ensuring public security", and Art. 16(2) codifies the protection of personal data. Consequently, the Court found Art. 82(1) TFEU as constituting an inappropriate legal base (para. 102), meaning that the agreement was (in its proposed form) not founded on the correct legal bases. In its argumentation, the Court aimed to strike a balance between the two fundamental purposes of PNR data transfer agreements, whilst also underlining the importance of a high level of personal data protection by declaring Art. 16 TFEU as a necessary legal base.

3.3.2. The compatibility with the rights to privacy and personal data protection

Within the second part of Opinion 1/15 the CJEU set legal precedence by ruling on the compatibility of an EU-third country agreement with the provisions of the CFREU, stating that whilst both Art. 16 TFEU and Art. 8 CFREU codify the protection of personal data, the Court would refer exclusively to the CFREU due to it including the "specific [...] conditions under which [personal data] may be processed." (para. 120). The CJEU initially stated that the proposed transfer of PNR data from the EU to Canada and the retention of such data *inherently* constituted an interference with the rights to privacy (Art. 7) and personal data protection (Art. 8) (para. 125-126), whilst subsequently noting that this interference could be justified (as they are not "absolute rights" (para. 136)). The Court found that owing to the purpose of the proposed agreement – the "protection of public security and safety" (para. 153) – the interference could be justified. This argumentation had far-reaching implications for PNR legislation both at the *internal* and *external* EU level, as the Court's proclamation underlined the fundamental legality of PNR data transfer agreements.

However, the Court noted that the justification of the interference in the above rights on the basis of the purpose of the agreement alone was not enough to confirm the agreements' compatibility with the Charter. Rather, according to the principle of proportionality (Art. 52(1) CFREU) the provisions regulating PNR data transfer in the draft agreement must also be "[...] limited to what is strictly necessary[...]." (para. 15), with the Court finding multiple provisions of the agreement as not fulfilling this requirement. Several of these provisions are of relevance concerning the further analysis involving the UK: firstly, the CJEU criticized the agreements provision on the retention of PNR data, specifically related to the continued retention of *all* PNR data after air passengers to whom these data belong had left Canada. The Court argued that since not *all* air passengers pose a security risk after they have left the country, the retention of PNR data of air passengers not constituting an evidence-based security risk after their departure "is not [...] limited to what is strictly necessary." (para. 206). Another relevant aspect of the Court's ruling was its emphasis on the concept of adequacy as the basis for personal data transfers from the EU to a third country (para. 214), which also relates to the Court's scrutiny of the agreements provision allowing Canada to transfer PNR data received from the EU to other third countries ("onward transfer").

Summarizing, on the grounds of both an incorrect legal base as well as the draft agreements non-conformity with the principle of proportionality to limit the interference into the rights of privacy and personal data protection to "what is strictly necessary" so as to fulfill the agreements' purpose, the CJEU invalidated the proposed EU-Canada PNR agreement. Moreover, it raised the bar on personal data protection which all EU-third country data agreements must adhere to. How the effects of these heightened standards materialize themselves in the EU-UK PNR provisions of the TCA is discussed in the next section.

3.4. Conclusion on the EU's third-country agreements on PNR data

Answering the second sub-question: "*To what extent is the EU allowed to share PNR data with third countries?"* is no straightforward task. On the one hand, the EU – both through legislation in the PNR Directive and GDPR, as well as through case law (Opinion 1/15) – has imposed strict limits on itself as to when and how it is allowed to share PNR data with third countries, with these limits designed to uphold the high standards of EU fundamental rights. On the other hand, the EU has not operated consistently within these limits, notably sacrificing higher standards on privacy and data protection in favour of increased (border) security whilst concluding the first EU-US PNR agreement. This aspect demonstrates how the EU has not always been able to assert its "normative power" over third countries, in times operating as a "norm taker" instead of a "norm maker". Considering these contradictions, it can be stated that *theoretically* the EU is only allowed to share PNR data with third countries as long as the requirements on the protection of privacy and personal data as laid out by the above regulations and case law are met, i.e. as long as the data exchange is compatible with the CFREU. However, *in practice* the EU seems to regard each third-country PNR data agreement individually (on a case-by-case basis), leading it to occasionally adopt PNR data agreements which – measured by the limits the EU sets itself – exceed what is "allowed".

4. The EU-UK PNR data transfer and the possibilities to diverge

After having addressed the internal and external EU dimension on data protection and PNR data, this final section introduces the "UK dimension", or more specifically, the EU-UK PNR data transfer under the TCA and aims to answer the sub-question: *To what extent could the UK – under the provisions of the TCA – diverge from EU standards and principles on data protection and PNR data transfers?* In order to answer this question, the section is split into two parts: initially, the regulatory framework governing EU-UK PNR data transfers is discussed, which includes the TCA's links to the EU's fundamental rights framework, the specific provisions on PNR data, as well as the UK's adequacy decisions. The second part contemplates the extent to which the UK could diverge from this framework and gain "PNR data autonomy". This means addressing current UK plans on data autonomy and discussing to what extent these plans could be realized behind the backdrop of the EU's regulatory framework and "normative power".

4.1. The regulatory framework governing EU-UK data protection and PNR

Only in the final days of the UK's formal EU-membership did the two parties conclude year-long negotiations on a comprehensive agreement, signing the "EU-UK Trade and Cooperation Agreement" (TCA) on the 30. December 2020. Having subsequently entered into force on the 1. May 2021, the TCA constitutes the main regulatory device governing "post-Brexit" EU-UK relations, with the largest part dedicated to trade-related provisions. However, the TCA is not solely a free-trade agreement, but also includes provisions on other areas of "cooperation", including on "Law Enforcement and Judicial Cooperation in Criminal Matters".

As noted by the European Data Protection Supervisor (EDPS) in early 2021, "[...] the TCA appears to be drafted based on the assumption that adequacy decisions under GDPR and LED will be granted [...]." (EDPS, 2021, para. 42). The EDPS was proven to be correct, as the Commission formally adopted two adequacy decisions (GDPR and LED) for the UK on the 28. June 2021, which "facilitate the correct implementation of the [TCA] [...]." (European Commission, 2021). The below sub-

sections discuss these adequacy decisions and TCA provisions, which together create the regulatory framework governing EU-UK data protection and PNR data cooperation.

4.1.1. TCA provisions on sovereignty and human rights

Several "general provisions" of the agreement must first be addressed, which relate back to both theoretical concepts underlying this thesis. Firstly, at the beginning of the TCA, several provisions underline the aspect of sovereignty: Art. 1 – codifying the TCA's purpose – enshrines each Parties' respect for the other's "[...] autonomy and sovereignty." (European Union, 2021). Furthering this notion, Art. 4(1) bases the TCA on "public international law" rather than domestic UK or EU law, with significant consequences: most notably, as emphasised "for greater certainty", this legal base means that both the EU's and the UK's court interpretations of the TCA are "not [...] binding on the courts of the other Party." (Art. 4(3)), thereby removing the CJEU's ability to pass rulings on the application of the agreement to which the UK would need to adhere. For the UK – long having sought freedom from the CJEU's power to overrule its parliament and therefore to undermine parliamentary sovereignty – the importance of this provision cannot be overstated.

The second aspect threaded throughout the TCA is the mutual commitment of both Parties to uphold and respect certain fundamental human rights and data protection standards, along with "shared values and principles of democracy" (Art. 763(1)). This commitment is of such importance that it is enshrined multiple times: In Title II of Part Six ("Basis for Cooperation"), the commitment is codified for the entire TCA, linking the respect for human rights to the UN's UDHR and declaring it an "essential element of the partnership" (Art. 771). Such a definition does not merely re-enforce *theoretical* importance, but also entails *practical* consequences, since Art. 772 regulates that in cases in which either Party finds "a serious and substantial failure" to have occurred in the fulfillment of any "essential elements", this Party has the option of suspending or even terminating the entire TCA (Art. 772(1)). Therefore, serious and substantive human rights violations by either Party could lead to the termination of the entire agreement. The Title also codifies the Parties' "commitment to ensuring a high level of personal data protection" (Art. 769), although this provision is notably not included in Art. 771's definition of "essential elements".

Furthermore, Title I of Part Three doubles down on both Parties' human rights commitment, mentioning not only the UDHR, but also the ECHR (Art. 524(1)). Beyond the explicit reference to the ECHR, the largest difference in Title I of Part Three compared to the "general provisions" of the entire TCA is found in Art. 525 on the "Protection of personal data". Whilst this provision repeats Art. 769's commitment to ensure high levels of personal data protection, it further defines specific rights and safeguards, many of which are "word-for-word" copies of those found in the GDPR (see section 2.1.), including lawful and fair data processing, data minimisation and purpose limitation, along with individual data rights such as erasure and rectification (Art. 525(2)). These similarities to the GDPR are striking and re-enforce both Parties' commitment to uphold the fundamental human rights to privacy and personal data protection throughout Part Three of the TCA, including in Title III (PNR). Furthermore, the near identical formulation of Art. 525's principles to those of the GDPR demonstrates the EU's strong stance in this area, indicating that the Union is unwilling to sacrifice its high *internal* standards on personal data protection in its *external* relationship with the UK, which relates back to the theory of "normative power Europe".

4.1.2. TCA provisions on PNR data

Title III of Part Three ("Transfer and Processing of Passenger Name Record Data") regulates the EU-UK PNR cooperation and thus constitutes a "third-country PNR agreement" akin to those the EU has previously adopted (e.g. US, Canada). The provisions (Art. 542 - 562 TCA) are largely based on the EU's *internal* PNR Directive (see section 2.3.), which leads to distinct similarities between the two acts, although notable differences also exist. Addressing the similarities, compared to the PNR Directive, the TCA provides for the same purpose (Art. 544(1)), the same data-sharing capabilities (UK competent authority sharing PNR data with Europol and EU Member-State PIU's) (Art. 546), the same prohibition of the processing of "special categories of personal data" (sensitive data) (Art. 548), as well as the same retention period (five years, de-personalization after six months) (Art. 552 (1,2)). Whilst this framework is shared between the Directive and the TCA, a closer analysis shows several (potentially impactful) differences: first, whilst the purpose of PNR data usage mirrors that of the Directive, Art. 544 TCA also provides for "exceptional cases", in which the UK can use PNR data *beyond the scope* of this purpose, such as in cases where "a significant public health risk" exists (Art. 544(2b)). More significantly, Art. 544(3) also permits "case-by-case" processing of PNR data if the necessity for doing so is determined "by a United Kingdom court". This exception – and especially the "one-sided" power of the UK to determine when to trigger such an exception – creates the possibility for the UK to *extend* its use of PNR data beyond the purposes' scope.

Furthermore, two relevant aspects can be found in Art. 543 TCA ("Definitions"): firstly, PNR – as defined by Art. 543(b) and Annex 40 – is conceptualised identically compared to the Directive, except for one significant aspect: point 12 of Annex I of the Directive ("General remarks"), which – as previously discussed (see section 2.3.2.) – has recently faced legal scrutiny by the CJEU, is *not* included in the TCA's Annex 40 and does therefore not constitute a PNR data element. This omission is a positive feature and demonstrates a higher level of personal data protection according to the principle of data minimisation as compared to EU's *internal* conceptualisation of PNR data. In reverse fashion however, Art. 543(f) TCA – defining serious crime – proves less comprehensive than its EU counterpart, as the Directive in Annex II includes an exhaustive "list of offences" which constitute serious crime (European Parliament/Council, 2016a, Annex II). The TCA defines serious crime as being any crime punishable with a prison sentence of "at least three years", most notably as laid out *exclusively* by the UK's domestic laws. Just as above, this "one-sided" provision greatly benefits the UK, since *both* Parties (EU and UK) are required to transfer PNR data so as to prevent serious crime, but only *one* Party (the UK) has the power to determine specifically how serious crime is conceptualised. Once again, this provision theoretically enables the UK to extend the use of PNR data further than the EU might like, i.e. to include crimes which the EU defines as "less serious".

The retention of PNR data (Art. 552 TCA) must also be addressed in more detail: whilst the general retention period of five years mirrors that of the Directive, Art. 552(4) regulates the duty of the UK to delete PNR data belonging to air passengers who have left the country, thereby relating back to and implementing a landmark decision on third-country PNR agreements stemming from the CJEU's Opinion 1/15 (see section 3.3.2.). Since deficiencies in this aspect contributed to the EU-Canada agreement's invalidation, the TCA's inclusion of this provision demonstrates the Parties acknowledgment of the CJEU ruling, which was welcomed by the EDPS (2021, para. 32). However, as stated in Art. 552(11), owing to "technical adjustments" necessary to enable the deletion of PNR data of departed air passengers, the UK can "derogate" from this duty for up to three years (Art. 552(13)), in which case the UK would begin deleting departed air passengers PNR data in 2024. The fact that the UK can (for three years) retain PNR data in a way which has been described by the CJEU as being

incompatible with the CFREU is a significant concession towards the UK and (temporarily) undermines the EU's standards on privacy and personal data protection.

Finally, Art. 556 TCA – regulating "Disclosure outside the United Kingdom", or "onward transfer" – needs addressing: a noteworthy positive is the detailed list of conditions which are required for the UK to be able to share PNR data with third countries, which includes the condition in Art. 556(1e) that the third country receiving PNR data from the UK must either have concluded a data protection agreement with the EU or posses an EU adequacy decision. Whilst Art. 556(2) does codify an exception to this condition, the requirements needed to "trigger" this exception – which include a "written assurance" from the third country to uphold the data protection safeguards prevalent in Title III of the TCA – ensure that onward transfer of PNR data is always subject to stringent safeguards. Especially through provision 1(e), the EU tries to limit the UK's "onward transfer" possibilities exclusively to third countries it "agrees" with, thereby emphasising the Union's efforts to prevent "uncontrolled" onward transfer of PNR data to third countries with lower personal data protection standards.

4.1.3. UK adequacy decisions

As previously mentioned, the TCA – with its commitment to human rights, data protection standards and frequent "word-for-word" transposition of GDPR provisions – was undoubtedly created on the assumption of adequacy being granted to the UK. The Commission in its press release on the 28. June 2021 confirmed this assumption, granting the UK adequacy both under the GDPR and LED. The press release states that "the UK has fully incorporated the principles, rights and obligations of the GDPR and the [LED] into its post-Brexit legal system." (European Commission, 2021). This opens the way for personal data to flow between the EU and the UK without additional safeguards and – more importantly – ensures the proper functioning of the TCA, as many of the provisions outlined above are inherently linked to the principles and standards of the GDPR and LED. However, the EU is not oblivious to the UK's desire for sovereignty in the area of data, having for the first time added an additional safeguard to an adequacy decision, which is designed to limit the extent to which the UK can diverge from the EU's standards on data protection. The safeguard – called a "sunset clause" – limits the duration of both adequacy decisions to four years, leading them to subsequently expire if not renewed. Such a safeguard is unprecedented in the history of EU adequacy decisions and demonstrates the Union's assumption that the UK could try to significantly diverge from "adequate" data protection standards. This "expectation" is reiterated by the Commission's Vice-President for Values and Transparency Jourová, who states that "[...] if anything changes on the UK side, we will intervene." (European Commission, 2021).

4.2. The UK's possibilities to diverge from the TCA's regulatory framework

On the 26. August 2021 the UK Government's "Department for Digital, Culture, Media & Sport" and its "Secretary of State" Oliver Dowden announced the UK's "post-Brexit global data plans" (UK Government, 2021a). These proposed measures are at the forefront of the UK's push for data autonomy from the EU and indicate the UK's plan to diverge from EU data protection standards and principles laid out in the TCA, which implicitly includes PNR-related provisions. The launch of these plans was met with concern from scholars and a widespread assumption that they would threaten UK adequacy under the GDPR and LED, with some scholars even declaring that "the UK's adequacy decision will almost certainly not endure." (Meyers/Mortera-Martinez, 2021, p. 4). In particular, the UK's plans to expand data usage for the purpose of increased economic growth – which include

planned data agreements with countries such as the US – could significantly undermine the protection of EU personal data in the UK and therefore lead to a loss of adequacy. This final sub-section discusses several aspects which could have a significant effect on the EU-UK PNR data exchange and considers the extent to which UK could implement them without risking the loss of EU adequacy or a suspension/termination of the relevant TCA Titles.

4.2.1. Economic conceptualisation of data

When discussing the UK's push for data autonomy, the starting point must be the specific conceptualisation of data which the UK is currently pursuing as opposed to the EU. Throughout all proposed changes to the current UK data regime, one central concept has emerged: the *economic potential* of data. This is illustrated throughout the proposed measures of the "post-Brexit global data plan", as well as in the previously released "Taskforce on Innovation, Growth and Regulatory Reform" (TIGRR) independent report, which contains proposals for the replacement of the UK GDPR with a new data framework enabling "[...] data to flow more freely and [to] drive growth [...]." (TIGRR, 2021, p. 49). The report describes "consumer data" – meaning personal data – as being "[...] highly profitable and a currency in itself." (2021, para. 205), which mirrors Oliver Dowden's comments that "[...] data is the 'oil' that will power 21st century Britain [...]." (The Telegraph, 2021). These descriptions speak towards the UK's conceptualisation of (personal) data as an economic tool/opportunity first and foremost, as opposed to the EU's understanding that the protection of personal data must always have priority. Furthermore, the importance of the UK's plans cannot be overlooked in regard to their symbolic value of the UK having managed to regain autonomy through Brexit, as Dowden stated that "creating our own data laws is one of the biggest prizes of Brexit."

4.2.2. AI and automated decision-making

Regarding specific proposals the TIGRR report sets out, "Proposal 7.2" suggests the removal of Art. 22 GDPR, which concerns "automated individual decision-making" and prohibits data subjects from being "[...] subject to a decision based solely on automated processing, including profiling [...]." (European Parliament/Council, 2016b, Art. 22(1)). The TIGRR report describes the economic benefits of using Artificial Intelligence (AI) in automated decision-making and suggests the removal or adaptation of Art. 22 GDPR "to permit automated decision-making and remove human review of algorithmic decisions." (TIGRR, 2021, para. 226). This proposal not only demonstrates the UK's willingness to "radically" diverge from EU data protection provisions, but also relates directly to the processing of PNR data: the CJEU in its recent judgment of C-817/19 addressed the "automated processing" of PNR data and stated that such processing may not be performed solely by AI-technology without human intervention (CJEU, 2022b, p. 3). AI-based processing of personal data is a highly sensitive matter and enables/eases the implementation of mass surveillance technologies such as the facial recognition systems used in China. Furthermore, automatic processing of personal data without human intervention poses significant threats to the GDPR's principles on data processing (Art. 5), in particular the requirement that data should be processed *transparently*. Therefore, it is unlikely the EU would tolerate any UK divergence from Art. 22 GDPR as suggested in Proposal 7.2, since such a divergence would enable the UK to subject EU individuals' personal data to AI-based automated processing and decision-making, thereby undermining key GDPR principles on data processing which safeguard the fundamental rights to data protection and privacy (Art. 7, 8 CFREU). Any

meaningful UK divergence from Art. 22 would therefore result in the loss of adequacy under the GDPR and significantly complicate EU-UK data exchanges and the functioning of the TCA.

4.2.3. UK global data partnerships and onward transfer

The UK is also ambitious to implement further plans which would have a significant effect on PNR data transfers, as can be seen in the proposed measures of the UK's "post-Brexit global data plans". These plans – which initially state that data is of fundamental importance not only for economic reasons, but also to "support law enforcement agencies tackling crime" – outline the UK's ambition to launch "new multi-billion pound global data partnerships with the US, Australia and [the] Republic of Korea", along with other countries such as Singapore, Colombia, India and Brazil. These new data partnerships are to be founded upon so-called "UK adequacy decisions", which the Digital Secretary would be able to adopt. Whilst the UK claims such adequacy decisions would be "[...] in line with our global ambitions and commitment to high standards of data protection." (UK Government, 2021b), they raise serious concerns over the level of protection of EU personal data in the UK, since – with the exception of the Republic of Korea - none of the above countries currently possess an EU adequacy decision, with the US having twice lost adequacy in the past two decades (EU-US Safe Harbour and Privacy Shield agreements). Onward transfer of EU personal data from the UK to these countries would therefore significantly threaten the standards and safeguards on privacy and personal data protection the EU strives to uphold. Furthermore, it can be expected that these proposed data partnerships will not be limited to the transfer/processing of personal data solely for economic purposes: a recent Statewatch article commenting on a UK consultation document called "Data: A new Direction" found it to include proposed reforms of the current UK data regime to "[...] remove certain distinctions between the general, law enforcement and intelligence data protection regimes [...]" (Statewatch, 2021). Such proposals are worrying, since they indicate the UK's ambition to diverge from the higher personal data protection standards the EU affords to the processing of personal data for law enforcement purposes. Regarding PNR, the previously discussed Art. 556 TCA regulates the onward transfer of EU PNR data by the UK, including the requirement that onward transfer of EU PNR data only be allowed to those third countries which themselves have been deemed as "adequate" by the EU (or possess a data agreement with the EU). As described by Meyers and Mortera-Martinez, "the countries the EU recognises as adequate [...] create a 'closed ecosystem' – they only recognise each other as adequate." (2021, p. 4). If the UK adopts PNR data-sharing provisions in its proposed global data partnerships with countries "outside" the EU adequacy ecosystem, it can be expected of the EU to react rapidly and stringently to prohibit the onward transfer of EU PNR data to these countries, which would certainly result in the loss of UK adequacy or even the suspension or outright termination of Title III of Part Three of the TCA.

4.3. Conclusion on the UK's possibilities to diverge from the TCA

Since leaving the EU the UK has rapidly advanced its plans to create an autonomous data regime, focussing mainly on economic goals and the (significant) GDPR diversions necessary to achieve them. A further signal of this push for autonomy was recently sent with the appointment of former New Zealand Privacy Commissioner John Edwards as the UK's new Information Commissioner, an appointment which Meyers and Mortera-Martinez describe as suggesting "[that] the UK wants [...] to achieve maximum divergence: maintaining EU adequacy but stretching adequacy to its limits.", since New Zealand – whilst possessing an EU adequacy decision – applies "less stringent" laws on

personal data protection as compared to the GDPR (2021, p. 3). However, due to the "sunset clause" of the UK's adequacy decisions, any significant "stretching" of adequacy would severely threaten a renewal after its automatic expiry. Furthermore, the UK is prepared to widen its global data approach, even to the detriment of safeguards and standards agreed upon with the EU in the TCA. Beyond this international scope, the UK retains the possibilities to expand the collection/use of PNR data nationally, as indicated by the specific TCA provisions discussed above. It remains to be seen how the EU would react to UK divergences from TCA provisions and GDPR principles, but recent precedence shows that the Union is unlikely to tolerate significant deviations. The EU has recently launched "new legal action" against the UK in reaction to its plans to diverge from TCA provisions on the "Northern Ireland Protocol" (BBC, 2022), demonstrating the EU's low tolerance for any UK breaches of TCA provisions.

There is further potential for regulatory discord in the near future as the EU's PNR Directive – on which the TCA provisions on PNR are largely based – recently faced new legal scrutiny by the CJEU (C-817/19), which Thönnes described as leaving the Directive "altered beyond recognition." (Thönnes, 2022b). If the EU and its Member-States therefore subsequently amend their *internal* framework on PNR so as to reflect this new ruling, it can be expected of the Union to also seek similar adjustments to its *external* PNR agreements, including the EU-UK PNR data transfer under the TCA. The willingness of the UK to consent to such amendments – thereby conceding indirectly to a CJEU decision – is doubtful at best. Summarizing, it seems likely the UK's current ambitions will lead to the loss of adequacy under the GDPR and LED, or at minimum the "non-renewal" of adequacy after its automatic expiration as per the "sunset clause". Whether the UK's plans will also lead to a suspension or even termination of TCA data-sharing provisions (including those on PNR data) is less sure, however – as illustrated above – the EU is not reluctant to take legal action when faced with a breach of TCA provisions. Therefore, answering the sub-question "*To what extent could the UK – under the provisions of the TCA – diverge from EU standards and principles on data protection and PNR data transfers?"*, it can be stated that the UK can only diverge from such principles and standards to the extent to which these divergences do not lead to a loss of EU adequacy or directly and significantly undermine TCA provisions. Specifically, this relates to any UK divergences which threaten the "principle of proportionality", as the CJEU recently reiterated that EU data mechanism (including PNR) must always be "limited to what is strictly necessary" (CJEU, 2022b, p. 1).

5. Conclusions

This thesis set out to answer the question *"To what extent does the post-Brexit "Trade and Cooperation Agreement" (TCA) allow the UK to develop an autonomous regime of data protection?"*. The question encapsulates the conflict between the two theoretical concepts underlying the thesis, the UK's push for sovereignty from the EU through Brexit vs. the normative power of the EU to export its high standards/safeguards on fundamental human rights through its third-country agreements. To illustrate this conflict, the thesis focussed on the specific issue of PNR data transfers, answering three sub-questions which led up to the thesis' main research question. The thesis initially analysed the regulatory framework governing *internal* EU PNR data transfers, before moving on to discuss the EU's *external* dimension of third-country PNR data agreements. This led to the discussion of the EU-UK PNR exchange under the TCA and finally the UK's plans to diverge from the TCA to create its own data regime. The thesis has shown that the EU – adhering to the concept of "normative power Europe" – aims to harmonize its *external* PNR agreements with its *internal* framework, especially towards securing high levels of personal data protection. However, the thesis also discussed how the

EU has not consistently managed to achieve this aim and has previously entered into third-country PNR agreements which did not afford "adequate" levels of personal data protection. Furthermore, the thesis has outlined the judicial challenges to PNR data, most notably the CJEU's landmark Opinion 1/15, which set a high benchmark for the EU's *external* PNR agreements, as well as Case C-817/19, which indicates that the EU's *internal* PNR Directive also requires amendment to conform with the fundamental rights of the CFREU. These findings are significant in many regards: they illustrate that the EU – whilst trying to harmonize its internal and external data legislation – does not always evoke true "normative" power. This indicates that the EU tries to balance its "export" of fundamental (data) rights with a desire for cooperation and a respect for its international (third-country) partners. Findings regarding the EU-UK data transfer however indicate that the EU is unwilling to compromise or allow for flexibility concerning certain aspects, most notably the "principle of proportionality" as relates to data.

It remains to be seen how determined the UK is to realise its ambitious data plans and how the EU will react to such divergences. Whilst precedence shows that the EU has in the past accepted "lower" standards on personal data protection in its *external* (PNR) data agreements, the Union's current attitude towards the UK suggests a "low-tolerance approach" to any significant breaches of TCA provisions. Providing an answer to the main research question, it can therefore be said that *in theory* the TCA severely limits the UK's possibilities of creating an autonomous data regime, to the point where a loss of UK adequacy would constitute the end of EU-UK data-sharing mechanisms (including PNR data) under the TCA. *In practice,* the EU will wish to avoid such a "collapse" and will therefore need to decide how many "sacrifices" on personal data protection standards it is willing to accept in order to continue cooperation. Current "anti-EU" sentiment in the UK and the symbolic importance of gaining (data) autonomy as proof of a "successful" Brexit seems to indicate that the UK is willing to push the EU "past its breaking point" and projects serious "de-regulation" in the future of EU-UK data exchanges.

6. Bibliography

Argomaniz, Javier. (2009). When the EU is the 'Norm-taker': The Passenger Name Records Agreement and the EU's Internalization of US Border Security Norms. *Journal of European Integration*, Vol. 31, Issue 1, pp. 119-136. https://doi.org/10.1080/07036330802503981. (last accessed 27/06/2022).

BBC. (2015). EU referendum: New 'exit' group launches its campaign. https://www.bbc.com/news/uk-politics-34482936. (last accessed 27/06/2022).

BBC. (2016). EU referendum: Time to vote for real change, says Boris Johnson. https://www.bbc.com/news/uk-politics-eu-referendum-35626621. (last accessed 27/06/2022).

BBC. (2022). EU takes new legal action against UK over post-Brexit deal changes. https://www.bbc.com/news/uk-politics-61809459. (last accessed 27/06/2022).

Bellamy, Richard. (2020). Taking Back Control: Demoi-cracy, Differentiation and the Role of National Parliaments. *IDEES*. https://revistaidees.cat/en/recuperar-el-control/. (last accessed 27/06/2022).

Citizens Information. (2021). Other EU data protection legislation. https://www.citizensinformation.ie/en/government_in_ireland/data_protection/legislation_relating_to_the_general_data_protection_regulation.html. (last accessed 27/06/2022).

Court of Justice of the European Union (CJEU). (2017). Opinion 1/15 of the Court (Grand Chamber).

Court of Justice of the European Union (CJEU). (2022a). Press Release No. 19/22 – Advocate General's Opinion in Case C-817/19. https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-01/cp220019en.pdf. (last accessed 27/06/2022).

Court of Justice of the European Union (CJEU). (2022b). Press Release No. 105/22 – Judgement of the Court in Case C-817/19. https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105en.pdf. (last accessed 27/06/2022).

European Commission. (2010). Communication from the Commission: On the global approach to transfers of Passenger Name Record (PNR) data to third countries.

European Commission. (2020a). The European Union: what it is and what it does. Publications Office. https://data.europa.eu/doi/10.2775/181831. (last accessed 27/06/2022).

European Commission. (2020b). Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. https://ec.europa.eu/home-affairs/system/files/2020-07/20200724_com-2020-305-review_en.pdf. (last accessed 27/06/2022).

European Commission. (2021). Data protection: Commission adopts adequacy decisions for the UK. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183. (last accessed 27/06/2022).

European Council. (2021). Regulating the use of passenger name record (PNR) data. https://www.consilium.europa.eu/en/policies/fight-against-terrorism/passenger-name-record/. (last accessed 27/06/2022).

European Court of Human Rights/Council of Europe. (2021). European Convention of Human Rights.

European Data Protection Supervisor (EDPS). (2021). Opinion 3/2021 – EDPS Opinion on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement.

European Digital Rights (EDRi). (2022). CJEU Advocate General states that PNR Directive does not violate fundamental rights despite mass surveillance concerns from civil society. https://edri.org/our-work/cjeu-advocate-general-states-that-pnr-directive-does-not-violate-fundamental-rights-despite-mass-surveillance-concerns-from-civil-society/. (last accessed 27/06/2022).

European Parliament/Council of the European Union. (2016a). Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. *Official Journal of the European Union* (L 119). European Union.

European Parliament/Council of the European Union. (2016b). Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union* (L 119). European Union.

European Parliament/Council of the European Union. (2016c). Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. *Official Journal of the European Union.* (L 119). European Union.

European Union. (2012a). Charter of Fundamental Rights of the European Union. *Official Journal of the European Union* (2012/C 326/02). European Union.

European Union. (2012b). Consolidated version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union* (C 326). European Union.

European Union. (2021). Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part. *Official Journal of the European Union* (L 149). European Union.

Given, Lisa M. (2008). The SAGE Encyclopedia of Qualitative Research Methods, (Volume 1 & 2). Thousand Oaks, CA. SAGE Publications, Inc.

Gstöhl, Sieglinde/Phinnemore, David. (2021). The future EU–UK partnership: a historical institutionalist perspective. *Journal of European Integration*, Vol. 43, Issue 1, pp. 99-115. https://doi.org/10.1080/07036337.2020.1818074. (last accessed 27/06/2022).

Haughton, Tim. (2021). It's the slogan, stupid: The Brexit Referendum. *University of Birmingham.* https://www.birmingham.ac.uk/research/perspective/eu-ref-haughton.aspx. (last accessed 27/06/2022).

Hobbing, Peter. (2008). Tracing Terrorists: The EU-Canada Agreement in PNR Matters. CEPS Special Report/September 2008. *Centre for European Policy Studies (CEPS).*

Kuner, Christopher. (2017). Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15. *Verfassungsblog.* https://verfassungsblog.de/data-protection-data-transfers-and-international-agreements-the-cjeus-opinion-115/. (last accessed 27/06/2022).

Manners, Ian. (2002). Normative Power Europe: A Contradiction in Terms?. *Journal of Common Market Studies*, Vol. 40, Issue 2, pp. 235-258. https://doi.org/10.1111/1468-5965.00353. (last accessed 27/06/2022).

Meyers, Zack/Mortera-Martinez, Camino. (2021). The Three Deaths of EU-UK Data Adequacy. *Centre for European Reform (CER).* https://www.cer.eu/sites/default/files/insight_ZM_CMM_data_15.11.21.pdf. (last accessed 27/06/2022).

Statewatch. (2021). UK: Plans to ease joint data processing by intelligence agencies, police and "national security partners". https://www.statewatch.org/news/2021/october/uk-plans-to-ease-joint-data-processing-by-intelligence-agencies-police-and-national-security-partners/. (last accessed 27/06/2022).

Tagesschau. (2013). Mit einem Fuß immer außerhalb der EU. https://www.tagesschau.de/ausland/eu-austritt100.html. (last accessed 27/06/2022).

Taskforce on Innovation, Growth and Regulatory Reform (TIGRR). (2021). Independent report. https://www.gov.uk/government/publications/taskforce-on-innovation-growth-and-regulatory-reform-independent-report. (last accessed 27/06/2022).

The Telegraph. (2021). Oliver Dowden: creating our own data laws is one of the biggest prizes of Brexit. https://www.telegraph.co.uk/politics/2021/08/25/oliver-dowden-creating-data-laws-one-biggest-prizes-brexit/. (last accessed 27/06/2022).

Thönnes, Christian. (2022a). A cautious green light for technology-driven mass surveillance: The Advocate General's Opinion on the PNR Directive. *Verfassungsblog*. https://verfassungsblog.de/green-light/. (last accessed 27/06/2022).

Thönnes, Christian. (2022b). A Directive altered beyond recognition: On the Court of Justice of the European Union's PNR decision (C-817/19). *Verfassungsblog*. https://verfassungsblog.de/pnr-recognition/. (last accessed 27/06/2022).

UK Government. (n.d.). Data protection. https://www.gov.uk/data-protection. (last accessed 27/06/2022).

UK Government. (2020). European Union (Withdrawal Agreement) Act 2020.

UK Government. (2021a). UK unveils post-Brexit global data plans to boost growth, increase trade and improve healthcare. https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase-trade-and-improve-healthcare. (last accessed 27/06/2022).

UK Government. (2021b). International data transfers: building trust, delivering growth and firing up innovation. https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers/international-data-transfers-building-trust-delivering-growth-and-firing-up-innovation. (last accessed 27/06/2022).

UK Parliament. (n.d.). Parliament's authority. https://www.parliament.uk/about/how/role/sovereignty/. (last accessed 27/06/2022).

United Nations. (1948). Universal Declaration of Human Rights.

Verovšek, Peter. (2020). Brexit and the misunderstanding of sovereignty. *Social Europe*. https://socialeurope.eu/brexit-and-the-misunderstanding-of-sovereignty. (last accessed 27/06/2022).

Wahl, Thomas. (2022). AG: PNR Directive is in Line with EU Charter. *Eucrim*. https://eucrim.eu/news/ag-pnr-directive-is-in-line-with-eu-charter/. (last accessed 27/06/2022).

Westcott, Nicholas. (2020). Sovereignty and Brexit: control of what exactly?. *UK in a Changing Europe (UKICE)*. https://ukandeu.ac.uk/sovereignty-and-brexit-control-of-what-exactly/. (last accessed 27/06/2022).