CHARLES UNIVERSITY

Faculty of Law

Tereza Pechová

International transfers of personal data outside the European Union

Master's thesis

Master's thesis supervisor: JUDr. Magdaléna Svobodová, Ph.D.

Department: Department of European Law

Date of completion (manuscript closure): 13. 12. 2023

UNIVERZITA KARLOVA

Právnická fakulta

Tereza Pechová

Mezinárodní předávání osobních údajů mimo Evropskou unii

Diplomová práce

Vedoucí diplomové práce: JUDr. Magdaléna Svobodová, Ph.D.

Katedra: Katedra evropského práva

Datum vypracování práce (uzavření rukopisu) : 13. 12. 2023

Declaration

I declare that I am the sole author of this submitted thesis, that all the sources used were properly cited and that the thesis was not used to obtain another or the same degree.

Furthermore, I declare that the actual body of this work has, including footnotes, 223 144 characters, including spaces.

Prohlášení

Prohlašuji, že jsem předkládanou diplomovou práci vypracoval/a samostatně, že všechny použité zdroje byly řádně uvedeny a že práce nebyla využita k získání jiného nebo stejného titulu.

Dále prohlašuji, že vlastní text této práce včetně poznámek pod čarou má 223 144 znaků včetně mezer.

Tereza Pechová

In Prague on/ V Praze dne

Acknowledgements

My sincere gratitude goes to the supervisor of this Master's thesis, JUDr. Magdaléna Svobodová, Ph.D., for her willingness and helpfulness in supervising this thesis, the attention she paid to the development of the thesis and her readiness to advise me at any point in the process of writing this thesis.

My thanks go to my friends and family for their care, thoughtfulness and endless support.

Table of Contents

Introduction 1

Research question 3

1. Development of the right to privacy and the right to personal data protection in the EU 5

1.1. Development of the right to privacy and the right to personal data protection 5

1.1.1. Materialization in international instruments for international data transfers 8

1.1.1.1. OECD Privacy Guidelines 8

1.2. Primary EU law 10

1.2.1. The Charter of Fundamental Rights of the European Union 11

1.2.2. Treaty of the Functioning of the European Union 12

1.3. Secondary EU law 13

1.3.1. Data Protection Directive 13

1.3.2. Personal Data transfers to third countries and adequacy of the level of protection under DPD 14

1.3.3. General Data Protection Regulation 16

1.4. Terminology used for personal data transfers under GDPR 18

1.4.1. Free movement of data 18

1.4.2. Data Flows 19

1.4.3. Data Transfers 19

1.4.4. The Data Processing Operation of Data Transfers 20

1.4.5. Data Transits 20

1.4.6. Third Countries 22

1.4.7. Special Territories of the EU 22

2. System of International Data Transfers available in secondary legislation (GDPR) 24

2.1. Data Transfers to third countries and adequacy of the level of protection under GDPR 26

2.1.1. Adequacy decisions 26

2.1.1.1. Personal data transfers on the basis of Adequacy Decision 27

2.1.1.2. Some of the important currently active positive Adequacy Decisions 30

2.1.1.3. The United States road to adequacy 32

2.1.1.4. Partial or sector-specific adequacy decisions 37

2.1.1.4.1. Canada's partial adequacy decision for private commercial companies 37

2.1.1.4.2. Japan as the first country with a mutual adequacy decision 38

2.1.2. Appropriate safeguards 39
2.1.2.1. Standard Contractual Clauses (SCCs) 39
2.1.2.2. Newer GDPR mechanisms: approved Codes of Conduct and accredited third-party certifications 42
2.1.2.3. Other Safeguards - Binding Corporate Rules 44
2.1.2.4. Derogations for specific purposes 44
2.2. Summary of the Chapter 45
3. International data transfer legal framework in the UK 47
3.1. The road to the UK Adequacy decision 47
3.1.1. Safeguarding the rights of Data Subjects 49
3.1.2. Adherence to rulings of the ECHR and CJEU 50
3.2. Brexit from the perspective of EU data protection law 51
3.2.1. The UK´s bargaining power to shape the EU-UK data protection relationship 53
3.2.2. Personal data protection during the negotiation period 55
3.2.3. The "Brussels effect" 57
3.2.4. A Bespoke Data Agreement or a Mutual Adequacy Decision? 58
3.3. The Trade and Cooperation Agreement 64
3.4. TCA Transitional Data Protection Arrangements 66
3.5. The UK Adequacy post-transition 67
3.5.1. Exemptions from the GDPR: Access to the personal data of EU citizens 69
3.6. An "Unstable" Adequacy Decision 69
3.6.1. Longer-term: continued alignment v divergence 73
3.7. Conclusion of the Chapter 76
Conclusion 78
List of common abbreviations 80
Bibliography 82
Title of thesis in Czech, abstract in Czech and keywords 98
Title of thesis in Czech, abstract in English and keywords 99

Introduction

In the current world, data is considered one of the most valuable currencies there is, and the oil of the technology sector. With the swift progression of technology and the Internet globally, a pressing need to establish a system of mechanisms to protect such valuable currency has emerged, especially pointing out the need to distinguish which of these sets of information need to be protected. For this purpose, various data protection systems have been launched around the world, deeming that personal data are the most precious and most in need of being protected. This led to the protection of personal data being included as a fundamental right in various legal orders around the world.

Personal data protection and privacy laws are a major challenge and a highly important topic in the current tech-dominated world, as the human population becomes more and more globalised, with the rise of digital platforms, cloud-based services, artificial intelligence services, social networks, and global companies. One of the most notable technological developments of the present time is Cloud Computing, impacting the "*complexity and volume of data flows globally*".[1] Based on the McKinsey Global Institute article, "*since 2005, the volume of data flows, measured in terabits per second, has multiplied by a factor of 45 in a decade, to reach an estimated 400 terabits per second by the end of 2016*".[2] As per the research conducted by McKinsey Global Institute in November of 2022, data has "*the fastest flow growth globally among intangible goods*", which even "*accelerated with the impact of the COVID-19 pandemic between the years of 2020 – 2021 and even reached an all-time high*".[3]

The massive growth of international data flow has led to an even higher need to be covered by adequate personal data protection legislation, primarily when the transfer of personal data occurs between countries with different approaches to personal data protection. As Yuko Suda jokingly claims in his publication, "*data may be collected in Berlin, processed in Bangalore, stored in Boston and accessed from Brisbane*".[4] This creates a problem of which legislation and mechanism shall be implemented on such transfers, as different countries have different stances

---

[1] SUDA, Yuko. *The Politics of Data Transfer: Transatlantic Conflict and Cooperation over Data Privacy (Routledge Studies in Global Information, Politics and Society)*. New York: Routledge, 2017. ISBN 1138696285, p. 1

[2] BUGHIN, Jacques a Susan LUND. *The ascendancy of international data flows.* Vox EU, McKinsey Global Institute [online]. 2017, 2017 [cit. 2023-08-03]. Available at: https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows

[3] SEONG, Jeongmin, WHITE, Olivia, WOETZEL Jonathan, SMIT Sven, DEVESA, Tiago BIRSHAN, Michael and SAMANDARI, Hamid. *Global flows: The ties that bind in an interconnected world: Discussion paper. McKinsey Global Institute* [online]. 2022, 2022 [cit. 2023-08-03]. Available at: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/global-flows-the-ties-that-bind-in-an-interconnected-world#/

[4] SUDA, op. cit. 1, p. 1

on the level of data protection. To ensure that the internet is not borderless per se, the increase of new data protection legislation has led to *a* "*significant rise in the personal data transfer mechanisms around the world.*"[5]

It is also necessary to note that data flows in said personal data transfers "*are not just binary from one country to another, but sequential (from one country to multiple countries) and therefore such transfers cannot be covered simply by conducting bilateral agreements between two countries*".[6] Such a regime would lead to an unsustainable amount of such bilateral agreements and is therefore dire to have wider and more complex data transfer mechanisms in place.

The European Union (the EU) has a fairly rigorous approach to personal data protection and, therefore, to international data transfers, compared to other regions or countries, which creates a need for international coordination to ensure an adequate level of personal data protection.

Yet, even if a third country's approach to data protection is very similar, for instance in the context of the United Kingdom (the UK) Data Protection legislation coming from the same origin, but beginning to differ after Brexit, a clear set of rules for such transfer must be in place to maintain the level of data protection afforded to the EU citizens. It is therefore intriguing to zero in on a case, where a country such as the UK, which left the European Union, deviates from EU legislation after a long joint development, and becomes a third country, having to bear the consequences of such a decision.

[5] JONES, Joe. *Infographic: Global data transfer contracts.* Iapp [online]. 2023, 2023 [cit. 2023-08-03]. Available at: https://iapp.org/resources/article/infographic-global-data-transfer-contracts/

[6] REINKE, Guido. *Blue Paper on Data Protection: Data Transfer between the European Union and third countries: Legal options for data controllers and data processors in a post-Brexit Britain,* London: GOLD RUSH Publishing, 2019. ISBN 1908585102, p. 7

Research question

This thesis focuses on international transfers of personal data and the depiction of an adequate level of protection that must be ensured when personal data are being transferred to and from the EU. In the thesis, the author aims to compare the means available to ensure such protection of international personal data transfers and to analyse which measures are being taken concerning transfers in the United Kingdom after leaving the EU due to Brexit. A deeper scrutiny of the UK in this thesis serves as a showcase of a country deciding to leave the EU and being no longer bound by the EU legal framework and is beginning to be considered as a third country within the EU data protection framework.

The thesis strives to examine, analyse, and assess in-depth the measures available to ensure an adequate level of data protection when a personal data transfer to a third country takes place. The thesis will address the provisions of EU law, related to transfers of data to a third country, in particular to the UK, a former Member State, now a third country. The Data Protection Directive, its successor, the General Data Protection Regulation, the concept of the adequacy of the level of data protection, and other instruments providing appropriate safeguards, are to be examined, as well as the available UK legislation and its evolvement after Brexit in comparison to the EU data protection framework.

The main focus of the thesis is to answer the research question of whether the UK, a former Member State with a transposed GDPR regime, has maintained the level of data protection regarding personal data transfers after Brexit. Furthermore, the thesis conducts a comparison of the UK GDPR and the current EU GDPR on this matter, as well as the measures currently in place and the discussions between the relevant data protection authorities regarding the future establishment of measures for personal data transfers. The purpose of the thesis is to answer the research question and to clarify the options and conditions when conducting international personal data transfers between the EU and the UK, using the tools of comparative analysis and synthesis, as well as reviewing the possible next steps in the future of such international data transfers and shedding light on the impact of such legislation and its development on international trade.

The thesis will mainly be pertaining to the general measures taken to protect larger data flows of personal data transfers performed by legal entities, such as global companies, concerning data flows of a larger volume, utilising the tools afforded by the GDPR, as opposed to international data transfers performed by an individual.

This thesis consists of an introduction, a description of the research question, and three chapters. These chapters will outline the privacy and data protection legal framework of the EU,

describe the systems of international data transfers, and analyse the legal framework of the UK post-Brexit, in comparison to the EU, regarding its impact on private entities as well as government authorities.

1. Development of the right to privacy and the right to personal data protection in the EU

1.1. Development of the right to privacy and the right to personal data protection

The European Union is a globally known pioneer with respect to the right to privacy and personal data protection and is known for its strictness when protecting individuals´ privacy and data protection rights. As of right now, the EU is leading data protection worldwide and is seen as the global "gold standard".[7]

The right to privacy, meaning the right to respect for private life, and the right to personal data protection are two distinct rights. However, they are closely related, as they both aim to protect similar values, "*i.e. the autonomy and human dignity of individuals, by granting them a personal sphere in which they can freely develop their personalities, think and shape their opinions.*"[8] As described in the Opinion of Advocate General Sharpston of joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, "*The EU deems both these rights to be essential for the exercise of other fundamental freedoms and rights such as freedom of expression, freedom of peaceful assembly and association, and freedom of religion.*"[9]

These rights, however, differ in both their scope and formulation. The right to privacy is a "*general right constituting general prohibition on interference*"[10] compared to the "*right to protection of personal data putting in place a system of checks and balances to protect individuals whenever their personal data are processed.*"[11] The right to personal data protection is applicable whenever personal data are being processed; it is thus in its scope broader than the right to respect for private life in this respect, meaning that data protection concerns in its scope all kinds of personal data and data processing, regardless of the relationship and impact on privacy.[12]

Both these rights were established on a constitutional level of the EU Member states. The right to the protection of personal data is also protected as a general legal principle based on the European Convention on Human Rights (ECHR) and the constitutional traditions of the Member

---

[7] *Handbook on European data protection law* [online]. 2018. Luxembourg: Publications Office of the European Union, 2018 Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-dataprotection_en.pdf, p. 3

[8] Handbook, op. cit. 7, p. 19

[9] Advocate General Sharpston described the case as involving two separate rights: the "*classic*" right to the protection of privacy and a more "*modern*" right, the right to data protection. *Joined cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston,* 17 June 2010, para. 71.

[10] Handbook, op. cit. 7, p. 18

[11] Ibid

[12] Ibid

States, including the Czech Republic. The EU provides a supranational standard to achieve a certain adequate level of protection for all EU Member states.

The right to respect for private life (right to privacy in terms of EU law) was first recognized in the Universal Declaration of Human Rights, adopted in 1948 as one of the fundamentally protected human rights. This was then followed by the European Convention on Human Rights (ECHR), drafted in 1950, which became a legally binding treaty on its parties. [13] The right to protection of personal data is an essential component of the rights safeguarded by Article 8 of the ECHR. The Article guarantees the right to respect for one's private and family life, home, and correspondence. It also sets out the circumstances under which limitations to this right are allowed.[14]

On the level of EU law, the right to private and family life can be found in the Charter of Fundamental Rights (CFR) of the European Union. The right to private and family life is contained in Article 7 of the ECHR, which states that "*everyone has the right to respect for his or her private and family life, home and communications.*"

Whilst the EU as a whole is not a party to the ECHR, all of its Member states are, leading to an alignment between the Court of Justice of the EU and the European Court of the Human Rights case law, in terms of fundamental human rights. [15] For example, in the case C-400/10 PPU J. McB v L.E the CJEU gave an interpretation of Article 7 of the Charter (corresponding to Article 8 ECHR). The court expressly stated that "*It is clear that the said Article 7 contains rights corresponding to those guaranteed by Article 8(1) of the ECHR. Article 7 of the Charter must, therefore be given the same meaning and the same scope as Article 8(1) of the ECHR, as interpreted by the case law of the European Court of Human Rights*".[16]

The ECtHR has made some landmark rulings on the matter of privacy and data protection rulings. Such rulings include, for example: *the regulation of eavesdropping powers*[17] (Case of Klass and Others v. Germany) *and mass surveillance*[18] (Big Brother Watch and others v. UK), *interception of telephone conversations*[19] (Malone v. United Kingdom) *blanket mobile phone*

[13] UNITED NATIONS GENERAL ASSEMBLY. *The Universal Declaration of Human Rights*, Paris, 10 December 1948, General Assembly resolution 217 A; COUNCIL OF EUROPE. *European Convention on Human Rights*, CETS No. 005, 1950
[14] Article 8 ECHR
[15] Handbook, op. cit. 7, p. 18
[16] Case C-400/10 PPU J. McB v L.E, ECLI:EU: C:2010:582, [2010]
[17] Klass and others v Federal Republic of Germany, Judgment, Merits, App no 5029/71 (A/28), (1979-80) 2 EHRR 214, IHRL 19 (ECHR 1978), 6 September 1978, European Court of Human Rights [ECHR]
[18] Brother Watch and Others v. the United Kingdom, App no 58170/13, 62322/14 and 24960/15, ECHR 2018, GRAND CHAMBER 2021, 25 May 2021 European Court of Human Rights [ECHR]
[19] CASE OF MALONE v. THE UNITED KINGDOM (Application no. 8691/79), Judgment Strasbourg 2 August 1984 European Court of Human Rights [ECHR]

interception devices[20] (Case of Roman Zakharov v. Russia), and *excessive collection of medical data*[21] (Case of L.H. v. Latvia).

The ECtHR rulings, however important they are, do not create a sufficient framework of data protection, as per the opinion of the Commission and its concerns about the privacy of the data being transferred from the EU to third countries. This is caused by the conflict between law enforcement and surveillance practices in third countries. Moreover, the ECtHR does not specify data processing and data transfers in its great amplitude.[22] Therefore, based on the above-mentioned, being a party to the ECHR is not in itself sufficient for having a fully functioning data protection framework.

The first mentions of personal data protection being distinguished from the right to privacy in Europe appeared in the 1970s aiming to control the processing of personal information by public authorities and large companies. By the 1980s multiple states such as France, Germany or Sweden have adopted some form of data protection legislation.[23]

Per Hustinx[24], "*the positive experiences with these first initiatives worked as a stimulus for the Council of Europe to invest time in the preparation of an international agreement as the first binding instrument on the subject."* This resulted in the adoption of the Data Protection Convention, known as Convention 108, which has been ratified by all EU Member States.[25]

The data protection standards in the European Union (EU) are established on the basis of the Council of Europe Convention 108 and several EU instruments, including the General Data Protection Regulation and the Data Protection Directive for Police and Criminal Justice Authorities. These standards are also influenced by the case law of the European Court of Human Rights and the Court of Justice of the European Union.[26]

The pioneer of the EU data protection secondary law was the Data Protection Directive (DPD) published in 1995, taking inspiration primarily from the OECD guidelines and the European Convention on Human Rights, helping form Articles 7 and 8 of the Charter.

---

[20] CASE OF ROMAN ZAKHAROV v. RUSSIA, App no 47143/06, JUDGMENT STRASBOURG, 4 December 2015, European Court of Human Rights [ECHR]
[21] L.H. v. LATVIA (Application no. 52019/07) JUDGMENT STRASBOURG 29 April 2014 FINAL 29/07/2014, European Court of Human Rights [ECHR]
[22] REINKE, op. cit. 6, p. 7
[23] HUSTINX Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation. New Technologies and EU Law.* Oxford University Press; 2017., p. 1
[24] Peter Hustinx is a former European Data Protection Supervisor, who has served in this role for 10 years and has been closely involved in the development of data protection law.
[25] HUSTINX, op. cit. 23, p. 1
[26] Handbook, op. cit. 7, p. 27-28

The DPD established a basic framework for the protection of personal information in the EU and was then replaced by the very well-known General Data Protection Regulation which became applicable in May 2018.[27]

1.1.1. Materialization in international instruments for international data transfers

Originating in the 1970s, rules on the transfer of personal data have been a significant component of data protection legislation since the early data protection laws in Europe. The very first international instruments for data protection were formulated in the 1980s. They were proposing an introduction of systems intended to facilitate and improve cross-border flows of personal data. In the European Communities, diverging rules on data transfers created many problems among the common market, thus the European Communities sought to harmonize the rules on data transfers with the Directive 95/46/EC in the 1990s.[28] Eventually, the EU consolidated these rules on an EU-wide level in 2016 with the GDPR, which will be addressed in the subsequent sections of Chapters 1. and 2.

The initial rules on data transfers in Europe created tensions, since there was a considerable opposition against restricting cross-border flows of personal data, due to their crucial role in communication, commerce, science, and many other human endeavours.[29] These tensions were one of the major objectives of the creation of international instruments, specifically intended to address the restrictions of data flows and their implications. The Organisation for Economic Co-operation and Development (OECD) drafted their Privacy Guidelines and the Council of Europe passed the Convention 108, both of which were supplemented with a model contract.[30]

1.1.1.1. OECD Privacy Guidelines

The steep increase in the number of national data protection laws, as well as different regimes and rules for transfers of personal data, caused major concern for international economic organizations, including the OECD, which focused their work on the field of data protection, to retain the ability to exchange personal data between member states in their Privacy Guidelines of 1980.[31]

---

[27] Handbook, op. cit. 7, p. 17

[28] NAEF, Tobias. *Data Protection without Data Protectionism The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*. Cham: Springer International Publishing, 2023. ISBN 3-031-19893-X, p.116

[29] PHILLIPS Mark. *International data-sharing norms: from the OECD to the general data protection regulation (GDPR).* Hum Genet 137(8):575–582, 2018, p. 575; PLOMAN Edward W., *International law governing communications and information.* Greenwood Press, Westport, 1982, p. 143, p. 228–232

[30] NAEF, op. cit. 28, p.116

[31] TZANOU Maria. *The fundamental right to data protection. Normative value in the context of counter-terrorism*

The OECD's approach towards transborder data flows is based on minimum standards for personal data protection and converging national data protection laws to avoid obstacles. The OECD Privacy Guidelines address transborder data flows in part three, stating that member states should:

i. "*consider the implication of their policies on processing and re-export of personal data for other member countries*"(Paragraph 15 OECD Privacy Guidelines);
ii. "*take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through member countries, are uninterrupted and secure*" (Paragraph 16 OECD Privacy Guidelines);
iii. "*refrain from restricting transborder flows of personal data to other member countries except where a member country does not yet substantially observe the OECD Privacy Guidelines or where the re-export of such data would circumvent a country's domestic privacy legislation*"(Paragraph 17 OECD Privacy Guidelines); and
iv. *"avoid developing laws, policies, and practices for the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data exceeding requirements for such protection*"(Paragraph 18 OECD Privacy Guidelines).

These paragraphs create a system, that, if implemented, allows for an unrestricted exchange of personal data between OECD member states. The explanatory memorandum outlines the system (in relation to Paragraph 17 OECD Privacy Guidelines) as providing "*a standard of equivalent protection, by which is meant protection which is substantially similar in effect to that of the exporting country, but which need not be identical in form or in all respects*".[32]

This was the first appearance of a concept similar to the standard of "*essential equivalence*".[33] The principles contained in the OECD Privacy Guidelines were designated to be the benchmark for the secure exportation of personal data. The OECD has cautioned against countries with weak data protection laws that ignore the principles outlined in the OECD Privacy Guidelines, as this affects the ability of other OECD member states to allow transborder data flows.[34] The OECD Privacy Guidelines also warned OECD member states against creating obstacles to transborder data flows, which would go beyond the requirements for the protection of

---

surveillance. Hart, Oxford, 2017, p. 15–16; NOUWT Sjaak. *Towards a common European approach to data protection: a critical analysis of data protection perspectives of the Council of Europe and the European Union*. In: Gutwirth S, Poullet Y, de Hert P et al (eds) Reinventing data protection? Springer, Heidelberg, 2009, p. 278; KIRBY Michael. *The history, achievement and future of the 1980 OECD guidelines on privacy.* Int Data Priv Law, 2011, p. 8

[32] OECD. *Explanatory Memorandum. Guidelines governing the protection of privacy and transborder flows of personal data.* Annex to the recommendation of the Council of 23 September 1980, para. 67

[33] NAEF, op. cit. 28, p. 121

[34] Paragraph 15 OECD Privacy Guidelines

personal data protection.[35] The OECD Privacy Guidelines were the first international instrument to formulate an international policy for data protection and were last amended in 2013.[36]

The OECD further released a Declaration on Government Access to Personal Data Held by Private Sector Entities, which was adopted by the OECD Members and the European Union, achieving an important milestone in addressing and promoting trust in cross-border data flows, as it was the first intergovernmental agreement in this area. The Declaration on Government Access to Personal Data Held by Private Sector Entities addresses a critical gap affecting cross-border flows of personal data - the lack of a common articulation of the safeguards that countries put in place to protect privacy and other human rights and freedoms when accessing personal data held by private entities for national security and law enforcement purposes.[37]

In 2017, The OECD also adopted the OECD Recommendation on Cross-Border Co-operation[38], mostly to address international cooperation among privacy law enforcement authorities, in order to better protect personal data and minimise disruptions to transborder data flows. The Recommendation is currently under review, as it has been 15 years since its adoption, to address changes that occurred since.

1.2. Primary EU law

Originally, there were no direct references to human rights in the treaties of the European Community, as their main purpose was simply to establish a common market.[39] The principle of conferral, on which the original treaties were based, only allowed for the European Communities even the EU as is right now, to act only within the limits of the competencies conferred upon it by the Member States.[40] The scope was then expanded by the CJEU rulings, which in multiple cases concluded an important interpretation of the treaties, alleging that human rights violations within the scope of EU law shall be regarded within the scope of EU law, granting protection to individuals. The CJEU then included the so-called fundamental rights into the general principles of European law. [41]

---

[35] Paragraph 18 OECD Privacy Guidelines
[36] OECD. *The OECD Privacy Framework: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines")*, revised recommendations, OECD Working Party on Information Security and Privacy, 2013; NAEF, op. cit. 28, p. 121
[37] OECD *Privacy. OECD.org* [online]. [cit. 2023-11-14]. Available at: https://www.oecd.org/digital/privacy/, OECD, *Declaration on Government Access to Personal Data Held by Private Sector Entities*, OECD/LEGAL/0487, [online]. [cit. 2023-11-14].
[38] OECD. (2023*) Review of the OECD Recommendation on Cross-Border Co-operation in the Enforcement of Laws Protecting Privacy*, OECD Digital Economy Papers, No. 359, OECD Publishing, [online]. [cit. 2023-11-14], Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487
[39] Handbook, op. cit. 7, p. 29
[40] Ibid
[41] Ibid

A great landmark for including personal data protection into the EU primary law was the adoption of the Lisbon Treaty in 2009, which provided a right to personal data protection and proclaimed the Charter of Fundamental Rights of the European Union legally binding. [42]

The inclusion of the right is also simultaneously reflected in the Treaty of the Functioning of the European Union, the purpose of which is explained in the following subsections 1.2.1. and 1.2.2.

1.2.1. The Charter of Fundamental Rights of the European Union

As per the EU Agency for Fundamental Rights: "*The signatories of the EU Charter commit to respect the right to private and family life, which public authorities may not interfere with, except in the interests of national security, public safety or the economic well being of the country or for the sakes of protecting the public health and the rights and freedoms of others*".

When discussing the right to personal data protection in the Charter of Fundamental Rights of the European Union, it is important to cite both Article 7 and Article 8 of said Charter. As aforementioned, Article 7 states the following: "*Everyone has the right to respect for his or her private and family life, home and communications.*" The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR.

The following Article 8 then goes on to specifically cover the aspect of personal data protection. Firstly, it proclaims that "*everyone has the right to the protection of personal data concerning him or her.*" Secondly, "*such 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. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified*." Lastly, it appoints that "*compliance with these rules shall be subject to control by an independent authority*". Article 8 is based on the Data Protection Directive as well as Article 8 of ECHR and Convention 108 as explained in the explanatory notes of the Charter.[43]

The case law related to the interpretation of the Charter is quite significant, as the interpretation of the Charter must be informed by the ECHR and its judicial interpretation. Likewise, the application must grant a level of protection at least equivalent to the one afforded by the ECHR.[44] This was interpreted by the ECtHR in multiple cases.[45]

---

[42] Ibid

[43] EUROPEAN CONVENTION. *Explanations relating to the Charter of Fundamental Rights*, OJ C 303, 14.12.2007, p. 17–35, Art. 8

[44] KAMARA, Irene, Eleni KOSTA and Ronald LEENES. *Research handbook on EU data protection law*. Northampton, MA: Edward Elgar Publishing, 2022, 1 online resource (664 pages). ISBN 1-80037-168-3., p. 15

[45] See, e.g., landmark rulings Leander v Sweden App no 9248/81 (ECtHR, 26 March 1987); Niemietz v Germany App no 13710/88 (ECtHR, 16 December 1992); Amann v Switzerland, App no 27798/95 (ECtHR, 16 February 2000).

1.2.2. Treaty of the Functioning of the European Union

The Treaty of the Functioning of the European Union provides the right to personal data protection in Article 16 of the TFEU. Article 16 TFEU is recognized as the foundation or the "*cornerstone provision*"[46] on the regulation of the protection of personal data across the EU, with its stipulation that "*Everyone has the right to the protection of personal data concerning them.*"[47] Article 16 TFEU establishes a clear rule on processing personal data by the EU institutions, bodies, offices and agencies and by the Member States when carrying out activities falling within the scope of EU law in relation to the free movement of personal data. These are regulated under the ordinary legislative procedure conducted by the EP and the Council, and it aims to ensure uniform application of rules in all areas of EU law when processing personal data.[48]

The article additionally creates a new basis for granting competence to the EU by establishing the right to legislate on data protection matters within the scope of EU law in its second paragraph.[49] Finally, the Article affirms the position of independent supervisory authorities regarding compliance with the adopted data protection rules in each Member state.[50]

Article 16 is crucial for the establishment of the free movement of data within the EU. The competence granted by the article allowed for legislation such as the Data Protection Directive and the General Data Protection Regulation to come into play.[51]

The TFEU also pays special attention to the issue of oversight in the area of personal data protection when assigning oversight of compliance with data protection rules to independent authorities. This is evident in Article 39, which makes use of a derogation foreseen in Article 16(2) TFEU in relation to common foreign and security policy. Article 39 TFEU establishes a special regime for the processing of personal data by the Member States when carrying out activities falling within the scope of common foreign and security policy. With regard to these issues, the Council is empowered to adopt a decision on the regulation of the processing of personal data in the area of common foreign and security policy. The Article only covers the Member States' processing of personal data, such processing in the area of common foreign and security policy by

[46] KAMARA, KOSTA and LEENES, op. cit. 44, p. 73
[47] Article 16(1) TFEU
[48] Ibid
[49] Article 16 TFEU „*The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data*."
[50] Article 16 TFEU „*Compliance with these rules shall be subject to the control of independent authorities*."
[51] Handbook, op. cit. 7, p. 28-29

Union institutions, bodies, offices, and agencies remains under the scope of Article 16 of the TFEU.[52]

1.3. Secondary EU law

The main objective of the secondary EU law regarding personal data protection is to provide harmonization among Member States, to ensure that each Member State reaches an adequate level of protection.[53] The aforementioned primary law provides the legal basis and grants competence to produce legislation (i.e. EU secondary law), which is able to achieve such an objective.

1.3.1. Data Protection Directive

The Data Protection Directive 95/46/EC32 came into effect in 1995 and was the first solution to ensure harmonization among Member states (as well as the following EEA members: Iceland, Liechtenstein, and Norway). The main focus of the directive was the achievement of a more balanced development of a free internal market in the EU.[54]

The DPD was first adopted before the existence of the Lisbon Treaty *under Article 100a of the Treaty of the European Community (then Article 95 TEC and now Article 114 TFEU) as an Internal Market measure.*[55] The CJEU addressed this in Rundfunk[56] and Lindqvist[57] and ruled Article 95 of TEC as the legal basis for DPD. The CJEU took the position that "*there is no need to have an actual link with free movement between Member States in every situation for the DPD to apply. What is important, held the Court, was that the measure, in these cases the DPD, shall have the intention to improve the conditions for the establishment and functioning of the Internal Market*".[58]

The DPD mainly covered two areas, the first being the protection of fundamental rights and freedoms of natural persons, in particular, the *right to privacy*[59] concerning the processing of personal data.[60] This again highlights the difference and relationship between the right to privacy and the right to personal data protection.

---

[52] KAMARA, KOSTA and LEENES, op. cit. 44, p. 73
[53] HUSTINX, op. cit. 23, p. 9
[54] Handbook, op. cit. 7, p. 29
[55] KAMARA, KOSTA and LEENES, op. cit. 44, p. 71
[56] Judgment of 20 May 2003, Österreichischer Rundfunk and others (C-465/00, C-138/01 and C-139/01, ECR 2003 p. I-4989) ECLI:EU:C:2003:294, [CJEU]
[57] Judgment of 6 November 2003, Lindqvist (C-101/01, ECR 2003 p. I-12971) ECLI:EU:C:2003: 596, [CJEU]
[58] Judgment of 20 May 2003, Österreichischer Rundfunk and others (C-465/00, C-138/01 and C-139/01, ECR 2003 p. I-4989) ECLI:EU:C:2003:294, [CJEU], para. 41.
[59] Recital 2 DPD
[60] HUSTINX, op. cit. 23, p. 9

The second area covered by the DPD established free data flow among member states and prohibited member states from restriction and prohibition of such data flows that are in accordance with the DPD.[61] The DPD also set up the establishment of independent supervisory authorities to exercise authority over compliance with the DPD over national legislation with several specific functions and powers, altogether to be exercised "*with complete independence*".[62]

The DPD drew from Convention 108 as well as existing national laws of several Member states.[63] It went on to clarify the principles and add further requirements and conditions, making it a more complex codification than ever before, whilst still allowing Member States a broad area of their own discretion in the transposition and implementation of the DPD.[64]

The directive established a detailed system of data protection in the EU. However, complete harmonization was not possible, due to the margin of discretion of transposing said directive by the Member states, which inevitably resulted in diverse data protection rules among the Member states, with both definitions and rules being interpreted differently in respective national laws. The enforcement and severity of sanctions also varied and were combined with the evolution of information technology since the drafting of the DPD. The aforementioned differences led to a need to reform the EU data protection legislation.[65]

To address these issues, the DPD set up the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (generally known as the "Article 29 Working Party")[66], which acted as an advisory body consisting of representatives of the supervisory authorities of each Member state until it was succeeded by the European Data Protection Board in 2018.[67]

1.3.2. Personal Data transfers to third countries and adequacy of the level of protection under DPD

The DPD states in Recital 56, that "*cross-border flows of personal data are necessary to the expansion of international trade*" and points out that the protection of the rights of individuals is not against the transfers of personal data to third countries, provided that third country fulfils the condition of "*ensuring an adequate level of protection*" as granted by the EU. To ensure the

[61] Ibid
[62] Article 28 DPD
[63] Handbook, op. cit. 7, p. 28-29
[64] HUSTINX, op. cit. 23, p. 9
[65] Handbook, op. cit. 7, p. 28-29
[66] Article 29 (1) DPD, Handbook, op. cit. 7, p. 28-29
[67] Ibid

adequate level of protection afforded by the third country, it must be "*assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations.*"[68]

Recital 56 is then followed by Recital 57, which established the rule that the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited.

The transfers of personal data to third countries are then further broken down in Chapter IV of the DPD entitled "Transfer of personal data to third countries". Article 25 entitled "Limitations" of said Chapter elaborates on Recital 56. The first paragraph of the article states that "*the Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if […] the third country in question ensures an adequate level of protection*".[69] The second paragraph then focuses on the assessment of the adequacy of the level of protection granted by the third county, taking into account "*circumstances surrounding a data transfer operation or set of data transfer operations, the nature of the data, the purpose and duration of the proposed processing operation or operations*, *the country of origin and country of final destination, the rules of law, in force in the third country in question and the professional rules and security measures which are complied with in that country*".[70]

Paragraph 3 of Article 25 DPD sets out a rule of compulsory communication between the Commission and Member States to inform each other when finding a country they do not consider to have an adequate level of protection as described in paragraph 2 of the Article.[71] If the Commission then finds that a third country does not ensure an adequate level of data protection (the procedure for such finding is described in Article 31 paragraph 2), the Member State is obliged to take measures to "*prevent any transfers of the same type to the third country in question*".[72]

On the contrary, based on Paragraph 6 of Article 25 DPD, the Commission is tasked with issuing adequacy decisions, meaning conducting an adequacy assessment, which if passed, leads to a positive adequacy decision, allowing for data to be freely transferred to a third country as if it was within the EEA. Allowing such transfers is crucial for the *expansion of international trade* as mentioned in the Recital 56 of the DPD. Adequacy decisions are not an exclusive condition for a third-country transfer; however, to allow transfers to such countries without adequacy decisions, additional safeguards must be provided. Article 26 DPD, titled "Derogations", provides a list of

[68] Recital 56 DPD
[69] Article 25(1) DPD
[70] Article 25(2) DPD
[71] Article 25(3) DPD
[72] Article 25(4) DPD

conditions to be followed when allowing a transfer to a third country without an adequacy decision.[73]

As the key principles of international personal data transfers have evolved and transformed with the adoption of the GDPR, the possibilities for data transfers in the absence of adequacy decisions will be addressed in detail according to current legislation in Chapter 2, describing the international data transfer system introduced by the GDPR.

1.3.3. General Data Protection Regulation

The General Data Protection Regulation, adopted in April of 2016, became fully applicable on 25 May 2018 (now referred to as the "*birthday of GDPR*") after years of intense discussions. It strived to address both the gaps in the previously adopted legislation such as the DPD as well as the technological development, which significantly progressed since the 1990s, when the DPD was adopted. After its adoption, the GDPR provided for a two-year transitional period, to allow the Member States to adjust to the new regulation. As the regulations under EU law are directly applicable, there was no need for national transposition, providing high legal certainty for data subjects across the EU.[74]

Together with the GDPR, the Directive (EU) 2017/680 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, was adopted.[75]

The adoption of the GDPR strived to modernise EU data protection as a whole, "*making it fit for protecting fundamental rights in the context of the digital age's economic and social challenges*".[76] The GDPR now introduces the "*protection of natural persons in relation to the processing of personal data is a fundamental right.*"[77] While preserving and developing the core principles and rights of data subjects (natural persons)[78] from the DPD, it introduced new obligations for organisations to implement data protection by design and default[79], to appoint a Data Protection Officer in certain circumstances[80], to comply with the principle of accountability or to comply with the new right to data portability.

---

[73] Article 26 DPD
[74] Handbook, op. cit. 7, p. 31
[75] Handbook, op. cit. 7, p. 18
[76] Handbook, op. cit. 7, p. 30
[77] Recital 1 GDPR
[78] Definition of a data subject can be found in Article 4(1) of the GDPR
[79] Article 25(1) GDPR
[80] Article 37 GDPR

When listing the most profound changes brought by the GDPR, the first to note is the definition of personal data as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*"[81] which substantially broadens the previous definition in the DPD.[82]

GDPR also introduced a list of new rights such as the "right of access"[83] providing data subjects with "*the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, as well as giving direct access to such data and information regarding the data, the right to the erasure of data*"[84] ("the right to be forgotten"), previously established by CJEU case law[85], "right to restriction of processing"[86], and "right to data portability".[87]

The regulation constitutes an opt-in opt-out regime of data processing, which translates to setting out the rules for consent to be regarded as a basis for lawful data processing in Article 6 GDPR (opt-in), requiring the data subjects' consent to be freely given, informed, specific and an unambiguous indication of wishes by a clear affirmative act signifying agreement to processing.[88] The data subject may withdraw such consent (opt-out) at any time.[89]

As for the right to the protection of personal data, the change compared to the DPD is the most obvious. The GDPR refers to this in the first sentence of the first recital. Data protection is no longer fundamentally based on market freedoms, but on an explicit unique right with its own legal basis in the primary EU law.[90]

Data transfers to third countries and the adequacy of the level of protection under GDPR shall be addressed in the next chapter, dedicated to the current system of international data transfers.

The right to data portability (RtDP) is also an integral part of the GDPR. It has long been a subject of many disputes as to whether it has been misplaced in the EU GDPR, as the Member

[81] Article 4(1) GDPR
[82] Article 2(a) DPD
[83] Article 15(1) GDPR
[84] Article 17 (1) GDPR
[85] CJEU, C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], 2014 CJEU, C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni, 2017
[86] Article 18 (1) GDPR
[87] Article 20 GDPR
[88] Article 7 GDPR
[89] Article 7(4) GDPR
[90] Recital 1 GDPR

States were inconclusive on whether this right is more of a consumer right than a data protection right and what should be done about its side effects on consumer welfare and competition. Concerns have also been voiced about its compatibility with the EU data protection framework. [91]

The RtDP seems more akin to the existing right of access, which predates the GDPR, and for that reason, it used to be treated as a subordinate right to the right of access. It appears not to further widen the purpose of personal data protection but another important objective of EU law, i.e. the free flow of personal data. It is criticised for its impracticability, as it does not, in itself, guarantee adequate coverage of data required to ensure smooth data migration. The right to data portability has clear potential, not yet fulfilled, to put individuals at the centre of the data economy. It can do this, by enabling users to switch between different service providers and to combine different services or to choose to use other innovative services or the most user-friendly data protection services, which would greatly benefit innovation and foster competition.[92]

1.4. Terminology used for personal data transfers under GDPR

The legal concept of data transfers is at the heart of the EU's fundamental rights-based data transfers regulation. The GDPR uses multiple terms when describing transfers of personal data from one place to another, such as the "free movement of data", "data flows", and "data transfers".

It is important to distinguish them, as the GDPR uses them in the context of data transfers without defining further what kind of data processing each operation entails, even though each term holds a different meaning.[93]

To better understand the mentioned terms in the concept of this thesis the author would like to shortly explain the terminology used when dissecting the broad topic of international data transfers.

1.4.1. Free movement of data

The first term the author would like to address is the "free movement of data". It refers to the passage or movement of personal data from one place to another in terms of EU data protection law. It is contained in the title of Directive 95/46/EC, which set out two objectives.. First to protect individuals with regard to the processing of personal data, and second to enable the free movement of this data.[94]

[91] KAMARA, KOSTA and LEENES, op. cit. 44, p. 572
[92] Ibid
[93] NAEF, op. cit. 28, p.136
[94] Directive 95/46/EC

Article 1(3) GDPR now refers to the "*free movement*" of personal data within the Union. Recital (13) of GDPR states that the free movement of personal data within the EU is necessary for the proper functioning of the common market. The term "free movement of data" therefore refers to data processing operations across the borders of EU member states.[95]

1.4.2. Data Flows

The term "Data Flows" is again used when referring to the passage of personal data from one place to another in EU data protection law. It was previously used in the OECD Privacy Guidelines and Convention 108 and the definition of instruments allowing free flow of data, reveals a data location-centric understanding of cross-border data flows.[96]

The GDPR also occasionally uses the term "data flows" when describing the passage of data across borders of EU Member States[97] and also sometimes to describe the passage of data outside the EU to third countries. [98] The term "data flows" refers to any cross-border transfer of personal data. It is a descriptive term and does not have legal implications like data transfers. This interpretation is consistent with Recital (101) GDPR[99] which indicates that out of all flows of personal data to third countries, there is a special category of transfers of personal data from the EU to third countries.[100]

1.4.3. Data Transfers

Arguably, the most important term of this thesis is "Data Transfers", which refers once again to the journey of personal data from one place to another in EU data protection law and is remarkably prominent, compared to the aforementioned. It indicates a sort of data processing operation, that carries with legal implications. The DPD had already used the term "Data Transfers" in Article 25 and Article 26. However, the term was not further defined in terms of the type of data processing operation it referred to. Indeed, an early draft of the GDPR, included an

---

[95] The use of the word "*move*" in Recital (116) GDPR describing data flows to and from countries outside the EU does not change the interpretation of "free movement of personal data." The French and the German versions are not consistent with the English version. They use other notions (franchissent and übermittelt) which do not correspond to the notion of free movement of personal data

[96] NAEF, op. cit. 28, p.136

[97] Recitals (3), (9), (10), (53), (123), (170) and Articles 4(24) and 51(1) GDPR

[98] See Recital (101) and Articles 58(2)(j) and 83(5)(e) GDPR. While the French version uses the same notion in these articles (flux de données), the German version uses the notion of data transfers (Datenübermittlung) which is better suited according to the differentiation suggested below because these articles refer to the legal concept in Chapter V GDPR. Article 8.81 of the Economic Partnership Agreement between the EU and Japan also contains a Rendez-vous clause according to which the two parties "*shall reassess within three years of the date of entry into force of this Agreement the need for inclusion of provisions on the free flow of data into this Agreement*."

[99] Recital (101) GDPR

[100] NAEF, op. cit. 28, p.136, ECJ, Lindqvist: ECJ, Judgement of 6 November 2003, Lindqvist, C-101/01, EU:C:2003:596, para. 71.

amendment that defined data transfers as "*any communication of personal data, actively made available to a limited number of identified parties, with the knowledge or intention of the sender to give the recipient access to the personal data*".[101] However, this definition was omitted from the final version of the GDPR.[102] Hence, the author would like to clarify the data transfer processing operation in the next section.

1.4.4. The Data Processing Operation of Data Transfers

As aforementioned, the transfer of personal data from the EU to a third country is deemed to constitute a specific data processing operation. The transportation of personal data to a destination in a third country is an appropriate description of the concept of the term "Data Transfers". It is important to note that using the terms "transfer" and "disclosure" interchangeably with regards to personal data can create problems when data flows do not involve direct access to personal information, such as in the case of cloud computing. Additionally, there is a reasonability test in place which limits the scope of data transfers and ensures the protection of fundamental rights.[103]

1.4.5. Data Transits

The term "Data Transits" is used when speaking of the routing of internet traffic, involving data flows passing through other countries before reaching their final destination in a third country. This passing through other countries before reaching the final destination is what is recognised as "Data Transits".[104] The GDPR does not mention the term and the DPD only referred to them through EU member states in Article 4(1)(c) DPD, as exceptions from the application of national data protection provisions. The UK Information Commissioner's Office published a guidance paper on data transfers in 2017 and stressed that "*transfer does not mean the same as mere transit*" because the ordinary meaning of transfer is transmission from one place to another.[105]

Christopher Kuner explained that the reason for exempting data transits from data transfers is that mere transits do not affect the rights and freedoms of individuals in the EU.[106] There is

The problem with this perception is that third country surveillance procedures are able to capture personal data in transit between the EU and another third country. Contrary to what Kuner

[101] Article 29 WP breaks up the definition of personal data into four elements. Personal data is information (1), relating to (2), an identified or identifiable (3) natural person (4). See Article 29 WP Opinion 4/2007 on the concept of personal data, 20 June 2007, p. 6
[102] NAEF, op. cit. 28, p.143
[103] Ibid, p. 143-144
[104] Ibid, p. 144
[105] ICO (2017) The eighth data protection principle and international data transfers. Version 4.1., 30 June 2017, para. 18
[106] KUNER Christopher. *Transborder data flows.* Oxford University Press, Oxford, 2013, p. 16

argued, the surveillance activities that occur when data travels across the network bridge, can still have an impact on the rights and freedoms of individuals in the EU. Given the infrastructure of the Internet, it is very tricky to identify the true route of data flows.[107] This is due to the structure of the Internet, which works in a way that the routing of data flows is based on technical parameters (such as latency, speed, thermal control) and not on geographical conditions.[108]

If the legal concept of data transfers were to apply to each case where personal data passes through a third country on its way to the destination country, the special regime set out in Chapter V of the GDPR would become a practically unfeasible solution for internet routing. If an "unavoidable" country (for technical internet routing) did not ensure adequate protection, a major amount of internet traffic from the EU would be prohibited. For instance, if the US was found to offer ensure inadequate protection of personal data and could not prevent data flows to other destinations, internet traffic from the EU containing personal data would be severely limited. Including data transits in the legal concept of data transfers would then have a huge impact on the internet as we know it today.[109]

The CJEU underlined in Lindqvist that it is necessary to take into account the technical nature of Internet transactions in order to apply the concept of data transfers.[110]

Through this line of argumentation, the CJEU has demonstrated a willingness to apply data protection law on the basis of technical facts, rather than to impose unreasonable requirements that would effectively make the internet impossible to operate. The author agrees with these arguments and deems that it would be unreasonable to prohibit a huge part of internet traffic from the EU, by including data transits in the legal concept of data transfers. It should be added that internet surveillance practices, which affect personal data in transit are relevant under international human rights law and raise possibilities of international action in order to safeguard not only the right to data protection in Article 8 CFR but also Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[111]

---

[107] "*Internet protocols have no notion of national borders, and interdomain paths depend in large part on existing interconnection business relationships (or lack thereof)*." EDMUNDSON A, Ensafi R, Feamster N, Rexford J (2016) Characterizing and avoiding routing detours through surveillance states. Princeton University, p. 1

[108] KUNER, op. cit. 106, p. 6.

[109] KUNER, op. cit. 106, p. 6.

[110] ECJ, Lindqvist: ECJ, Judgment of 6 November 2003, Lindqvist, C-101/01, EU:C:2003:596, para. 57.

[111] HON Kuan W. *Data localization laws and policy. The EU data protection international transfers restriction through a cloud computing lens.* Edward Elgar, Cheltenham, 2017, p. 311

1.4.6. Third Countries

The term "Third Country" permeates the concept of international transfers of personal data in the EU law. From the GDPR´s point of view, all countries that are not EU member states are generally considered "Third Countries". The only exceptions are member states of the Agreement on the European Economic Area: Iceland, Liechtenstein, and Norway.[112] Together with the EU Member States, the EEA member states form a common market. Given the importance of data protection and free movement of data for the functioning of the common market, the DPD has been considered EEA-relevant and was incorporated into Annex XI of the Agreement on the EEA in 1999.[113] On 6 July 2018, the EEA Joint Committee decided to update Annex XI and incorporate the GDPR into the Agreement on the EEA as the successor to the DPD, making the Agreement on the EEA a basis for free movement of personal data within the EEA, just as in the EU. Iceland, Liechtenstein, and Norway are therefore not considered third countries within the meaning of Articles 44-49 GDPR.[114]

The European Commission makes decisions on whether data protection laws in third countries are adequate, in accordance with Article 25 of the Data Protection Directive. This includes a few regions that are not independent countries but have a form of self-government that includes data protection laws. One of the examples is the Faroe Islands.[115] It has been argued that these decisions are based on the fact that these places exercise sovereignty with respect to data protection law. The "territory" adequacy decision option in the GDPR applies to these locations without expanding the concept of a third country.[116]

1.4.7. Special Territories of the EU

The special territories of the EU are territories of EU member states that have a special status within the EU, for either historical, geographical, or political reasons. The EU recognizes nine outermost regions (OMR) that form part of the EU including the Azores, French Guiana, La Réunion, and the Canary Islands[117] and 13 overseas countries and territories (OCT) that do not

---

[112] Agreement on the European Economic Area of 2 May 1992 [1994] OJ L 1/3
[113] EEA Joint Committee (1999) Decision No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement, [2000] OJ L 296/41, EEA Joint Committee (2018) Decision No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement, [2018] OJ L 183/23
[114] NAEF, op. cit. 28, p.142; KRZYSZTOFEK, Marius. *Post-Reform Personal Data Protection in the European Union. General Data Protection Regulation (EU) 2016/679*. Kluwer, Alphen aan den Rijn, 2017, ISBN 9789041162427, p. 167
[115] "*According to the European Commission, the Faeroe Islands are a self-governing community within the Kingdom of Denmark that did not join the EU when Denmark did*." Cp. European Commission (2003b), Recital (5).
[116] NAEF, op. cit. 28, p.142
[117] Article 355(1) TFEU

form part of the EU, though they cooperate with the EU via the overseas countries and territories association including Greenland, French Polynesia, and Aruba.[118]

Finally, there are a few special cases. For instance, Guernsey, Jersey and the Isle of Man, self governing islands under the UK jurisdiction, are considered a third country for the purposes of the GDPR, have their own adequacy decision, which is addressed in the following chapter.

In comparison, the OMR and OCT are usually not considered third countries for the sake of the GDPR. For instance, in France, the national adaption of the French law to the GDPR entails extensions of the GDPR to the French OCT such as in French Polynesia and the Wallis and Futuna Islands.[119]

Data flows to the OMR and the OCT do not constitute data transfers to third countries. Instead, they fall under the free movement of personal data according to Article 1(1) of the GDPR. The free movement of personal data to the OMR and the OCT may, however, involve data transits. As mentioned before, the transfer of data may be subjected to surveillance practices which can have an impact on the rights and freedoms of individuals in the European Union. However, the GDPR permits the free movement of personal data, including to the OMR and the OCT, even if such data transfers affect the rights and freedoms of individuals in the EU. This is clearly stated in Article 1(3) GDPR: "*The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data*."[120]

Article 1(3) GDPR implies possible limitations on the right to continuous protection of personal data in Article 8 CFR when data transits to the OMR and the OCT are subject to surveillance practices of third countries. AG Henrik Saugmandsgaard Øe accepted the risk that a third country other than the destination country may secretly intercept data flows from the internet infrastructure while the data are in transit in his opinion on the Schrems II judgement.[121]

[118] Article 198 TFEU and Annex II TFEU; NAEF, op. cit. 28, p.145

[119] Titre V Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés; CNIL (2019); TAMBOU, Olivia. *The French adaptation of the GDPR*. In: McCullagh K, Tambou O, Bourton S (eds) National adaptations of the GDPR. Blogdroiteuropéen, Luxembourg, 2019, p. 53

[120] NAEF, op. cit. 28, p.145

[121] ECJ, AG Opinion, Schrems 2: ECJ, Opinion of AG Saugmandsgaard Øe delivered on 19 December 2019, Schrems 2, C-311/18, EU:C:2019:1145, para. 237

2. System of International Data Transfers available in secondary legislation (GDPR)

Data is the oil of the information economy and the lynchpin for the exploitation of high-tech opportunities in data science in the 21st century. As mentioned before, data flows are not binary from one country to another (say for example the Czech Republic to the UK) but sequential (say from Brazil to the UK to Switzerland) and therefore cannot be solved by bilateral agreements. This is reflected in Article 44 of the GDPR as any transfer to a third country or to an international organisation shall take place only if the conditions of Chapter V of the GDPR on Transfers of personal data to third countries or international organisations as well as Article 50 of the GDPR are met. This calls for development of international cooperation mechanisms to facilitate the effective enforcement of legislation for the protection of personal data, mutual international assistance in the enforcement of legislation for the protection of personal data, engagement of relevant stakeholders in discussion and activities aimed at furthering international cooperation in the enforcement of legislation for the protection of personal data and promotion of the exchange and documentation of personal data protection legislation and practice.[122]

At the same time, data flows present one of the greatest trials for preserving human autonomy and privacy. The challenges of enabling cross-border data flows and protecting personal data at the same time cannot be solved on a national level. It is not only a question of harmonising legislation but more importantly making regulatory decisions in response to specific issues surfacing due to the rise of new technologies on an ongoing basis. This requires constant ongoing exchanges between regulatory authorities in different countries, which is impossible to perform on an ad-hoc basis, but only within frameworks of trust and mutual recognition. The transition to digital economy and the increasing importance of (personal) Big Data ought to suggest a recognition of the fifth freedom[123] of the European Single Market (or Internal Market): *the free movement of data*.[124]

The EU's legislative competence in the area of free movement of data is based on the EU's competence in the area of the internal market. The EU's competence under Article 16 II TFEU is based only on the free movement of personal data, while the legislative competence concerning non-personal data can only be based on Article 114 TFEU. The free movement of personal data is

[122] Art 50 GDPR
[123] The "*Four Freedoms*" of the European Single (Internal) Market or also the EU Internal Market are: the Free Movement of Goods, Services, Capital and Labour.
[124] REINKE, op. cit. 6, Foreword by professor Julia Hörnle, Queen Mary University – Data Flows require trust an mutual recognition, p. vii

a protected right of the GDPR and a framework for the free flow of non-personal data has been established by the "Free Flow of Data" Regulation 2018/1807, which primarily prohibits data localization rules of EU Member States. From the perspective of data protection law, it would be interesting to see what the outcome would be if the right to free movement of data were incorporated in the primary law of the EU.

Politically speaking, the right to free movement of data has been the EU's goal for years. The impact of including the free movement of data into TFEU would widen the scope set by Article 16 II of the TFEU, and from the author´s point of view would mean further unification of both personal and non-personal data protection in relation to international data transfers and the EU Internal Market. It would also widen the scope of the CJEU jurisdiction with regard to questions on the Internal Market now including free movement of data. The impact of such a provision would be enticing for third countries wanting to join the EU and third countries with adequate safeguards in relation to international trade, as the provision would grant them automatic free flow of data in the Internal Market of the EU as a whole.

The EU exercises free flow of data within the EU Member States as well as the EEA, and EFTA States as described in the previous chapter, as these countries have adopted the GDPR, recognized as the golden standard for personal data protection. "*The GDPR sets stricter standards in regards to the territorial scope of data transfers. In the context of EU data protection, this has been rather about evolution than a revolution.*"[125]

The GDPR provides solutions for countries outside of the free flow of personal data regime, meaning that personal data can be transferred to a third country, a territory or one or more specified sectors within the third country or an international organisation if they fulfil one of the options of appropriate safeguards offered by the GDPR. A third county, a territory or one or more specified sectors within the third country or an international organisation must meet an adequate level of data protection before transfers of data are made to this country, sector or organisation, without ongoing authorization.

This chapter will focus on the assessment of legal options for international data transfers offered by the GDPR and also focus on the regime of the UK as a former EU Member State and its solution for personal data transfers post-Brexit.

[125] REINKE, op. cit. 6, p. 21

2.1. Data Transfers to third countries and adequacy of the level of protection under GDPR

Article 46 of the GDPR abandons the presumption under Directive 95/46/EC, that personal data may not be transferred if there is no "*adequacy level of protection in the recipient country*" and constitutes that as long as the conditions set out in the provisions of the GDPR are met, the transfers are feasible.[126] The three mechanisms offered for allowing data transfers are listed herein: Commission adequacy decisions (Art. 45 GDPR), the use of "Appropriate Safeguards" (Art. 46 GDPR), including Binding Corporate Rules (Art. 47 GDPR) or lastly certain enumerated Derogations (art. 49 GDPR).[127] Article 45 of the GDPR allows for Adequacy decision-making to be even more flexible by widening its scope beyond just countries, to include specific "territories" or specified "sectors" within a third country or an international organisation. Article 50 of the GDPR encourages the Commission and Member States' Supervisory Authorities to cooperate internationally for the protection of personal data, recommending specific steps. [128]

2.1.1. Adequacy decisions

Adequacy decision are a formal determination made by the European Commission on whether a non-EU country can ensure an adequate level of personal data protection in accordance with the EU law once international data transfer takes place.

Once a positive adequacy decision is granted, personal data may freely flow from Member States of the EEA to non-EEA country/countries without any further or alternative safeguards. For the UK, this was the ultimate goal when negotiating the post-Brexit personal data protection framework and the trade negotiations with the EU after leaving, making it the ultimate solution to maintain its trade relationships and secure a free flow of personal data.[129]

An adequacy decision puts the countries' organisations who control data – data controllers and/or process – data processors in a position to transfer personal data with no or no significant contractual agreements between several legal entities involved.[130] For determining whether a country should be awarded a positive adequacy decision, the Commission utilises analysis of current arrangements of countries, that obtained such positive adequacy decisions, to spot possible weaknesses and explain possible further challenges, that may be faced with future adequacy

[126] Art 46 GDPR
[127] Art 46 GDPR
[128] Art 50 GDPR
[129] REINKE, op. cit. 6, p. 31
[130] Ibid, p. 33

decisions. For this purpose, current adequacy decisions are analysed. The current active adequacy decisions concerned are the following adequacy decisions for Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay as providing adequate protection.[131]

With the exception of the United Kingdom, these adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive (Article 36 of Directive (EU) 2016/680).[132] The United Kingdom adequacy decision will be examined in depth in the next chapter.

The Commission´s aforementioned adequacy decisions simultaneously cover international (business) organisations, however they are not automatic or guaranteed for big-name global firms such as Dell, BT, RBS, Facebook and others. On one hand, Vera Jourova the EU Commissioner for Justice, Consumers and Gender Equality, who was in charge of data protection stated in 2019 "*We definitely will want for the sake of business interests the quickest and most efficient legal framework for the exchange of data with the UK*".

On the other hand, Giovanni Butarelli, Europe's data protection supervisor at that time (EDPS) has warned against the impact of Brexit as Brexit would be a "*personal data protection Brexit*". This issue seems to be resolved for now, with the adequacy decision currently in place, with possible alternatives. If the route of an adequacy decision fails the UK would be required to take an accountability approach, which would provide incentives for data controllers not to circumvent EU rules.[133]

2.1.1.1. Personal data transfers on the basis of Adequacy Decision

The Commission is tasked, under the GDPR, with conducting the adequacy assessments of personal data protection of a third country or an international organisation. The GDPR allows the Commission to decide whether a third county, a territory or one or more specified sectors within

[131] European Commission. *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection*. In: EUROPEAN COMMISSION. Commission.europa.eu [online]. 2023, [cit. 2023-10-19]. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[132] Ibid

[133] KUNER, Christopher. *Developing an Adequate Legal Framework for International Data Transfers*. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds) Reinventing Data Protection?. Springer, Dordrecht., 2009, ISBN 978-1-4020-9497-2, p. 10

the third country or the international organisation in question ensures or does not ensure an adequate level of protection based on Article 45(2) GDPR. [134]

Article 45(2) and Recital 104 of the GDPR provide a list of criteria for an adequate level of protection of personal data transferred to or through third countries or international organisations, fulfilment of which, exempts them from the need for specific authorisations for such transfers. The adequacy criteria include the following: i) the rule of law, human rights and fundamental freedoms, reckoning in the effect of the law of public security and public order, defence and national security, and crime ii) effective independent data protection supervision to enforce the law and to provide a mechanism for cooperating with EU Member States´ data protection authorities, and adequate means for data subjects to enforce their rights, if necessary through the judicial redress, and iii) legally binding agreements and/or participation in "multilateral or regional systems" to protect personal data.[135]

The key consideration of the Commission´s adequacy assessment is whether or not the third country has acceded to the Council of Europe's (CoE´s) Convention 108, to which all the Member States of CoE are parties as well as non-member states which have received a white-list (adequate) status (such as Argentina, Morrocco and Uruguay). The importance of the CoE conventions and protocols to the GDPR scheme is such that the Council decision of April 9 of 2019 authorised the EU Member States to ratify the latest modernisation of Convention 108, namely the Protocol Amending the Protection of Individuals with regard to Automatic Processing of Personal Data of 10 October 2018 (CETS No. 223), now largely accomplished. In addition to most EU countries, CETS No. 223 has also been ratified by Andorra, Iceland, Monaco, Norway, the Russian Federation, and others. This gives these signatories an inside track to a positive adequacy decision by the Commission.[136]

If these criteria are met, an adequacy decision can be granted to a third country, a territory or a specific sector within this third country or an international organisation, so as to ensure an adequate level of protection.[137]

It should be noted that adequacy decisions are not permanent. The Commission is bound to monitor developments in third countries and other subjects on an ongoing basis, at least once every four years. It is important that this review considers the conclusions of the EU Parliament,

---

[134] Article 45(2), Recital 104 GDPR
[135] Ibid
[136] COUNCIL OF EUROPE. *Chart of signatures and ratifications of Treaty 223*. In: Council of Europe. Coe.int [online]. 2023, [cit. 2023-10-19]. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223; REINKE, op. cit. 6, p. 34
[137] Art 45(3) GDPR and Recital 104 GDPR

the European Council and other relevant organizations. The findings should then be reported to the Article 93 Committee, a comitology group established by the EP and the Council to work together with the Commission in implementing the GDPR (as outlined in Article 45(3) and Recital 106 of the GDPR). The full assessment procedure is explained in Art 93(2) GDPR, this article refers to EU Reg No. 182/2011 "*laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission´s exercise of implementing powers".* If adequate protection cannot be ensured, the adequacy decision can be repealed, amended or suspended (Art 45(5) GDPR). Remediation steps should be agreed upon (Art 45(6) GDPR). This could happen for example if the UK repeals the GDPR or breaches the criteria of their adequacy decision.[138]

The Commission´s assessment cases are made public. In the past the process of awarding an adequacy decision was not transparent, although some knowledge of the criteria was available, assessments were not treated like EU tender evaluations, where clear criteria and weighing for each criterion is provided as a part of the process. Adequacy decisions were often political, based on the need to support economic and political relationships and trade, often neglecting enforcement and redress in the case of failure to safeguard personal data.[139]

Kuner stated in 2019 that the EU's legal framework for personal data transfers outside the EU was inadequate and needed reform. He criticized the process of adequacy, which requires costly and lengthy procedures. The under-sourcing at the relevant units of the Commission is one of the reasons for this. The process is also influenced by political factors, making the outcome unpredictable. Moreover, only a relatively small number of countries have received a positive adequacy decision, primarily small countries on a "white list". He deemed that to be due to the lack of tools and "best practices", absence of standardised checklists, clear procedures, and deadlines for the various steps in reaching a positive adequacy decision. He finds there is also a need for partial or sectoral adequacy decisions, which would reduce the complexity and increase the speed of the process of granting an adequacy decision.[140]

For the upcoming future of the adequacy decision assessment and granting process, per the author´s opinion, it would be beneficial for the GDPR to undergo reform. Such reform should lead to assuring that the Commission amends the process, particularly to make it more transparent regarding the criteria as well as informing third countries or organisations of the reasons for not granting them a positive adequacy decision. This would imply that the countries, previously

[138] REINKE, op. cit. 6, p. 34
[139] Ibid
[140] KUNER, op. cit. 133, p. 10

awarded a negative assessment, can improve their data protection framework to be essentially adequate in the sectors where they are lacking. A good example of such a situation would be India, which has been rejected multiple times without proper justification of the relevant reasons for not receiving a positive adequacy decision. Such amendment should be the author´s opinion regularly updated and published for parties interested in acquiring positive adequacy decisions and not remain a hidden cabinet process done internally and guarded from the public by the European Commission.

2.1.1.2. Some of the important currently active positive Adequacy Decisions

Some of the issues of lack of transparency, and the criteria being unclear when granting an adequacy decision, still persist nowadays. Despite the improved technology and communications on the Commission´s website, very little has been done to improve the transparency of the process and the final evaluation criteria used for adequacy decisions. This highlights the importance of analysing and reviewing current active adequacy decisions such as those described below[141]:

Andorra was the first country ever to be put on a white list to receive a positive adequacy decision as Andorra has enshrined a right of privacy in Article 14 of its Constitution. Moreover, Andorra has ratified the Protocol amending the Convention 108 – CETS No. 223. Its legal rules for personal data protection in the Qualified Law 15/2003 are based on the EU Directive 95/46/EC. [142] The Andorran Data Protection Agency, an independent body separated from the Andorran government, has investigatory powers and therefore judicial remedies are guaranteed (EC Andorra Adequacy, 19 October 2010).[143]

Argentina has implemented general and sector-specific rules as laid down in its Constitution and Data Protection Act, transforming personal data protection into a constitutional right. This shows that adequacy does not require an alignment to EU data protection law but only a determination that the relevant protections are implemented and enforcement instruments are made available to data transfer subjects. The Commission´s Decision (EC Argentina Adequacy, 30 June 2003)[144] stressed that an important consideration in its assessment of adequacy was that "*Argentina´s constitution makes privacy a fundamental right*".[145]

---

[141] REINKE, op. cit. 6, p. 35-36
[142] Ibid
[143] 2010/625/EU: *Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra*, Official Journal L 277, 21.10.2010; REINKE, op. cit. 6, p. 35-36
[144] 2003/490/EC: *Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina,* Official Journal L 168, 5.7.2003
[145] REINKE, op. cit. 6, p. 35-36

Guernsey, Jersey and the Isle of Man, the three self-governing islands in the English Channel and the Irish Sea, associated often with the UK are in fact outside UK jurisdiction. Though not members of the EU, they have a special relationship to it, with regard to their access to the Customs Union (Guernsey is also part of the Single Market). All three islands have ratified the Convention 108 and have enacted a data protection framework based on the standards set out in the Directive 95/46/EC. Each island has an independent Data Protection Commissioner (EC Guernsey adequacy, 21 Nov 2003[146], EC Isle of Man adequacy, 28 April 2004[147], EC Jersey adequacy, 8 May 2008[148]). These decisions show that the Commission puts some weight on a robust international legal framework.[149]

Like the UK, Israel lacks a written constitution, but has a large body of case law and related basic non-constitutional laws. In conjunction with the Israeli Privacy Protection Act and decisions by the government as well as financial and health sector-specific regulation, the Commission has deemed Israel EU-adequate[150] (EC Israel adequacy, 31 January 2011).[151]

New Zealand also does not have a written constitution, but the Commission's decision highlights the importance of human rights in the context of personal data protection. The Bill of Rights Act 1990, The Human Rights Act 1993, and the Privacy Act 1993 are specifically mentioned in the decision. This indicates the value the Commission places on protecting human rights concerning personal data protection[152] (EC New Zealand adequacy, 19 December 2012).[153]

Switzerland has well-defined data protection laws at both Federal and Cantonal levels, with a Federal Commissioner possessing the authority to investigate and intervene (EC Switzerland adequacy, 26 July 2000)[154]. It is clear from this decision that the Commission wants to see "*not*

---

[146] 2003/821/EC*: Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey*, Official Journal L 308, 25.11.2003; REINKE, op. cit. 6, p. 35-36

[147] 2004/411/EC: *Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man,* Official Journal L 151, 30.4.2004; REINKE, op. cit. 6, p. 35-36

[148] 2008/393/EC: *Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey*, Official Journal L 138, 28.5.2008

[149] REINKE, op. cit. 6, p. 35-36

[150] Ibid

[151] 2011/61/EU: *Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data*, Official Journal L 27, 1.2.2011; REINKE, op. cit. 6, p. 35-36

[152] REINKE, op. cit. 6, p. 36-37

[153] 2013/65/EU: *Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand*, Official Journal L 28, 30.1.2013; REINKE, op. cit. 6, p. 35-36

[154] 2000/518/EC: *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland*, Official Journal L 215, 25.8.2000; REINKE, op. cit. 6, p. 35-36

just law on the books but also a forceful regulator fully equipped with the authority to enforce it".[155]

2.1.1.3. The United States road to adequacy

The urgency and need for the Safe Harbor framework and an adequacy decision between the EU and the US was first insinuated after the adoption of the Data Protection Directive and the Safe Harbour decision, which was agreed between the EU and the US in 2000. It was challenged in 2013 by privacy campaigner Max Schrems, which resulted in declaring the Safe Harbour agreement invalid by the CJEU in 2015 in the Max Schrems v. Data Protection Commissioner case (The Court (Grand Chamber) Judgement, 6 October 2015 – "Schrems I")[156]. The Safe Harbour framework was deemed inadequate by the CJEU in 2015 due to a lack of "essentially equivalent" protection to that provided in the EU, resulting in the invalidation of the Commission's adequacy decision.[157]

The complaint was lodged with the Irish DPA following the transfer of data to the US by Facebook´s European HQ in Ireland. Schrems argued that the US government did not sufficiently protect European citizen´s data from state surveillance (such as the PRISM surveillance programme). The CJEU ruled in 2000 that Safe Harbour was sufficient. However, following the Snowden revelations in 2015, the High Court of Ireland sought guidance from the European Commission to determine whether it could overrule the CJEU's decision.[158] The CJEU determined that public interest and law enforcement regulations in the US can override Safe Harbour, if there is a conflict found between these two, hence its new ruling has made data transfers under Safe Harbour unlawful. As an aftermath of the decision, major international companies such as Google, Microsoft, Apple and Facebook were no longer able to rely on self-certification but had to take refuge in standard contractual clauses to authorise data transfers outside of EU. [159]

After the Court declared the Safe Harbour regime, both the EU and the US proceeded to negotiate a new framework that would hold up to the requirements of EU law and the Court's findings, as the establishment of a functional data protection framework for personal data transfers was crucial between the two sides of the Atlantic. At the beginning of February 2016, the

---

[155] Ibid
[156] Case C-362/14 Schrems I. ECLI:EU:C:2015:650 [2015]
[157] Case C-311/18 Schrems II. ECLI:EU:C:2020:559 [2020]
[158] In 2013 Edward Snowden revealed that the UK´s Government Communications Headquarters (GCHQ) was secretly storing, processing and intercepting the data of millions of people's private communications, although to no intelligence interest (the "Tempora Programme") - HARDING, Luke, *The Snowden Files: The inside story of the world's most wanted man*, Vintage Books, 2016, ISBN-100804173524
[159] Case C-311/18 Schrems II. ECLI:EU:C:2020:559 [2020]

Commission announced an agreement on a new framework for data flows to the US. The new framework promised "*commitments that US authorities' access to personal data transferred will be "subject to clear conditions, limitations and oversight, preventing generalised access.*"[160]

The Safe Harbor agreement was invalidated by the CJEU for two main reasons. Firstly, it was found that legislation existed which allowed for generalized access to electronic communication content. Secondly, the legislation did not provide individuals with any means of pursuing legal remedies to access, rectify, or erase their data.[161]

The Privacy Shield came into effect on August 1 2016 and included a number of changes regarding data protection, including the following: i) companies that receive personal data from EU data subjects will have stronger obligations. These will include regular reviews and updates, and limitations on sharing data with third parties, ii) the US government will be subject to certain safeguards and transparency obligations when accessing data (to rule out indiscriminate mass surveillance on personal data transferred), iii) there will be a redress mechanism for citizens whose data have been misused (including an Ombudsman mechanism and Alternative Dispute resolution) and iv) a yearly review mechanism will be conducted by the US Department of Commerce and the Commission to oversee the agreement.[162]

Personal data access was expanded, with data minimalization principle for retention. With certain exceptions, organizations now could retain data only "*as long as it serves a purpose of processing*" and no longer indefinitely, such as was the case under Safe Harbor. In case of an onward transfer, the third-party organization had to provide the same level of protection as the forwarding subject. Additionally, data subjects gained the right to opt-out of the disclosure of their data to a third party (with limited exceptions).[163]

In relation to private entities, the Privacy Shield framework improved certain aspects of the Safe Harbor framework, but the structural issues remained. A lack of meaningful, effective, and independent redress offered to EU data subjects was still present regarding private entities It resulted in a complicated system of parallel procedures and limited enforcement options that required individuals to carry out non-compliance cases in the US court system.[164]

---

[160] EUROPEAN COMMISSION. EU *Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield* [online]. IP/16/216. Strasbourg. 2016. [cit. 2023-10-20]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216

[161] Case C-362/14 Schrems I. ECLI:EU:C:2015:650 [2015], para 94 and 95

[162] EUROPEAN COMMISSION. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield [online]. IP/16/216. Strasbourg. 2016. [cit. 2023-10-20]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216

[163] Ibid

[164] REINKE, op. cit. 6, p. 39

Following the former complaint of Maxmillian Schrems and the subsequent Schrems I. ruling of the CJEU, the matter returned to the Irish Data Protection Authority (the Commissioner), re-opening the investigation, and requested Schrems to reformulate the original complaint, as the Safe Harbor decision was no longer valid. Essentially, like in the first case, the complaint was based on the operation of mass surveillance programs and the absence of judicial remedies.[165]

Consistent with the opinion of privacy NGOs and the European Data Protection Supervisor, the Privacy Shield framework did not pass the scrutiny of the CJEU as a result of the Schrems II ruling[166], as the criteria and requirements laid down in Schrems I., were not compatible with just the framework itself but with the US surveillance regime as a whole. Even though the US tried to take steps to overcome the EU´s data protection and privacy concerns, there was very little room for considerations on whether the declared safeguards were in fact being followed. Simultaneously, the safeguards do not fundamentally change the nature of the US surveillance regime, which clearly contradicts the proportionality and acceptable interference requirements of EU legal regimes.[167]

As an immediate consequence, organisations had to rely on Standard Contractual Clauses and other more limited means (such as Binding Corporate Rules or Codes Of Conduct) to enable international personal data transfers with the EU. The transfers had to adhere to the criteria laid down in the Schrems II. judgement, namely providing additional safeguards. If they had failed to do so, it would have meant an end to such data flows to the US.[168]

On March 25th, 2022, the US and the Commission jointly announced a new agreement in principle to replace Privacy Shield: "*Trans-Atlantic Data Privacy Framework*".[169] According to the press release, "*the United States is to put in place new safeguards to ensure that signals surveillance activities are necessary and proportionate in the pursuit of defined national security objectives, establish a two-level independent redress mechanism with binding authority to direct remedial measures, and enhance rigorous and layered oversight of signals intelligence activities to ensure compliance with limitations on surveillance activities*".[170] The aim of the new framework

---

[165] Data Protection Commissioner v. Facebook Ireland Ltd and Schrems [2017] IEHC 545, para 28 and 30
[166] Case C-311/18 Schrems II. ECLI:EU:C:2020:559 [2020]
[167] EUROPEAN COMMISSION. Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo [online]. STATEMENT/21/1443. Brussels. 2021. [cit. 2023-10-20]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443
[168] Case C-311/18 Schrems II. ECLI:EU:C:2020:559 [2020], para 134
[169] EUROPEAN COMMISSION. *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo* [online]. STATEMENT/21/1443. Brussels. 2021. [cit. 2023-10-20]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443
[170] Ibid

is to ensure safe and secure data flows through a durable and reliable legal basis to protect the data flows valued at approximately €900 billion in cross-border commerce every year.[171]

On July 10, 2023, the European Commission (EC) adopted its long-awaited adequacy decision approving the EU-U.S. Data Privacy Framework (DPF). By doing so, the EC confirmed that personal data transferred to the United States under the DPF is adequately protected in line with the rules on international data transfers imposed by the EU General Data Protection Regulation.[172]

The European Commission has approved the EU-U.S. Data Privacy Framework (DPF) for transferring data from the EU to the United States which meant that after the failure of both Safe Harbour and Privacy Shield, the US has once again gained a positive adequacy decision.[173]

The DPF however can only be used for transfers of personal data to the United States, while the SCCs can be used to transfer personal data from the EU to any non-EU country. When using the SCCs, other compliance requirements still apply. There are substantial differences between the SCCs and the DPF in terms of the upfront investment required and the ongoing compliance burden. The organisations that need to transfer personal data from the EU to the United States are now faced with an important decision: Does it make sense to use the DPF that only applies to data transfers to the US, or is it better to leverage one of the other transfer tools available under the GDPR, such as the EU's Standard Contractual Clauses?[174]

The EU has taken a leading role in respecting privacy and human rights, and many countries and businesses around the world have basically implemented EU principles.[175] The GDPR's wide territorial scope requires US businesses to comply with EU rules when offering services to EU customers and collecting their data. Compared to the US, the UK´s continued alignment to the EU framework played a big factor in easing the adequacy arrangements with third

---

[171] EUROPEAN COMMISSION. Factsheet: Trans-Atlantic Data Privacy Framework [online]. Brussels. 2022. [cit. 2023-10-20]. Available at: https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/TransAtlantic%20Data%20Privacy%20Framework.pdf.pdf

[172] GREAVES, Paul a Wim NAUWELAERTS. *Privacy, Cyber & Data Strategy Advisory: EU-U.S. Data Privacy Framework vs. EU Standard Contractual Clauses for Transatlantic Transfers of Personal Data*. *ALSTON&BIRD* [online]. USA: ALSTON&BIRD LLP., 2023, 5 [cit. 2023-10-20]. Available at: https://www.alston.com/en/insights/publications/2023/09/eu-us-data-privacy-framework

[173] 2023/1795/EC: Commission Implementing Decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework notified under document C(2023) 4745, Official Journal of the European Union OJ L 231

[174] GREAVES, Paul a Wim NAUWELAERTS. *Privacy, Cyber & Data Strategy Advisory: EU-U.S. Data Privacy Framework vs. EU Standard Contractual Clauses for Transatlantic Transfers of Personal Data*. *ALSTON&BIRD* [online]. USA: ALSTON&BIRD LLP., 2023, 5 [cit. 2023-10-20]. Available at: https://www.alston.com/en/insights/publications/2023/09/eu-us-data-privacy-framework

[175] WEBER, Rolf H. a Dominic STAIGER. *Transatlantic Data Protection in Practice*. Zurich, Switzerland: Springer, 2017. ISBN 3662572338, p. 22

countries which have adopted EU principles.[176] "*At the global level, the EU's involvement in multilateral bargaining is shaped by its relationship to the US. The two great trade powers have been engaged for years in what the rest of the world sees as a battle of titans, whereby each side tries to ensure a continued balance in market access to the other side through trade and regulatory deals*."[177] Compared to the UK, is an important market as well, but comparably has far less bargaining power compared to the US and is economically way more dependent on the EU.[178]

Concerning the UK framework for international data transfers there is a new UK-US Data Bridge, effective as of 12 October 2023, which provides a solution for UK-US data transfers. The Secretary of State has determined that the UK Extension to the EU-US Data Privacy Framework does not undermine the level of data protection for UK data subjects when their data is transferred to the US and the decision was based on their determination that the framework maintains high standards of privacy for UK personal data. The decision was taken under the scope of under Section 17A of the Data Protection Act 2018. The Secretary of State has determined that the UK Extension to the EU-US Data Privacy Framework does not undermine the level of data protection for UK data subjects when their data is transferred to the US. [179]

The Data Bridge is a preferred UK public terminology for an adequacy decision between the concerned countries, which describes the decision to permit the flow of personal data from the UK to another country without the need for further safeguards. The UK-US Data Bridge establishes a data bridge for the "UK Extension to the Data Privacy Framework", allowing certified US companies to sign up to be able to receive UK personal data through the mentioned framework.[180]

Adequacy regulations have been laid in the UK Parliament today on 21 September 2023 to give effect to this decision. UK businesses and organisations are able to make use of this data bridge to safely and securely transfer personal data to certified organisations in the US from 12 October, when the regulation came into force. Supporting this decision, the US Attorney General, on 18 September, designated the UK as a 'qualifying state' under Executive Order 14086. This allows all UK individuals whose personal data has been transferred to the US under any transfer mechanisms (i.e. including those set out under UK GDPR Articles 46 and 49) access to the newly

[176] Ibid, p. 3
[177] MEUNIER, Sophie and COLAIDIS, Kalypso. *The European Union as a conflicted trade power*. Routledge, Taylor&Francis Group. 2006, p. 911
[178] REINKE, op. cit. 6, p. 40
[179] GOV.UK. *UK-US data bridge: explainer: Notice.* In: Gov.uk [online]. UK, s. 1 [cit. 2023-11-14]. Available at: https://www.gov.uk/government/publications/uk-us-data-bridge-supporting-documents/uk-us-data-bridge-explainer
[180] Ibid

established redress mechanism in the event that they believe that their personal data has been accessed unlawfully by US authorities for national security purposes. [181]

2.1.1.4. Partial or sector-specific adequacy decisions

The Commission has adopted a tough stance on privacy in international trade[182] as respecting privacy is a condition for stable, secure and competitive global commercial flows. As the Commission has stated: "*Privacy is not a commodity to be traded*".[183] Canada has been deemed to provide only partially adequate protection, which is analysed in the following section. Historically the US framework also provided only partial adequacy, however, that has now changed, as the new EU-US Data Privacy Framework is now in place.

2.1.1.4.1. Canada's partial adequacy decision for private commercial companies

In Canada, only private organizations covered by the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) and using personal data for commercial activities have access to personal data from the EU under the Commission's adequacy decision. This adequacy decision also supports the Comprehensive Economic Trade Agreement (CETA) that was negotiated between the EU and Canada. In its decision, the Commission deemed the Canadian Act adequate (EC, Canada (commercial organisations) adequacy, 20 December 2001)[184], although it only applies to private sector organizations that disclose personal data outside Canada and it exempts the public sector, employment data, and data used for non-commercial purposes. The European Commission also emphasized that Canada has officially adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (29 June 1984, revised in 2013) and the UN Guidelines Concerning Computerized Personal Data files (14 December 1990).[185]

Following Brexit, Canada and the UK concluded the Canada-United Kingdom Trade Continuity Agreement, which entered into force on April 1 2021, preserving preferential market access for both Canadian and UK businesses.[186]

---

[181] Ibid
[182] EC, 14 October 2015:7
[183] REINKE, op. cit. 6, p. 37
[184] 2002/2/EC: *Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act*, Official Journal L 2, 4.1.2002
[185] Ibid
[186] GOVERNMENT OF CANADA. *The European Union's General Data Protection Regulation.* Tradecommissioner.gc.ca [online]. 2023, [cit. 2023-10-03] Available at:

2.1.1.4.2. Japan as the first country with a mutual adequacy decision

On 17 July 2018, Japan became the first foreign state which has counter-vetted the EU for data protection adequacy. The Commission and Japan successfully concluded negotiations on mutual adequacy of data protection.[187] The reciprocal recognition was made in the context of the EU-Japan Economic Partnership Agreement (EPA). EPA was finalised on 23 January 2019 and entered into force on 1 February 2019. The Agreement underlines[188] the importance of free data flows for the export of goods and services.[189]

This was not only the first adequacy decision granted on the basis of the GDPR (it came into force 25 May 2018), but per Věra Jourová (EC Commissioner for Justice, Consumers and Gender Equality) it also "*created the world's largest area of safe data flows*".

To be considered adequate, Japan had to implement additional safeguards before their data protection regimes was recognized as equivalent to the EU.[190] The additional safeguards included: i) additional rules to bridge the difference between the two data protection regimes, which will be enforced by the Personal Information Protection Commission (PPC), Japan´s data protection authority, and by the Japanese courts, and covering the protection of sensitive data, the enforcement of individual rights and upholding of the safeguarding rules under the aegis of which EU personal data may be transferred from Japan to a third country, ii) a complaint-handling mechanism operated by the PPC to investigate and properly dispose of complaints from EU Data Subjects, iii) guarantees that Japanese public authorities will be restricted from accessing personal data for criminal law enforcement and national security purposes through mechanisms of independent oversight and redress.[191]

Japan implemented the Act on the Protection of Personal Information (APPI) which came into force on 30 May 2017, however, it still provided inadequate personal data protection, so to achieve adequacy the aforementioned safeguards and modifications had to be implemented. Graham Greenleaf, analysing the mutual adequacy decisions of the EU and Japan identified a mix of criteria forming the basis of adequacy assessments. These derive partly from the GDPR, from CJEU´s decisions on the Schrems I and Schrems II cases, and the Art 29 WP Opinions.

---

https://www.tradecommissioner.gc.ca/guides/gdpr-eu-rgpd.aspx?lang=eng

[187] European Commission. "*The European Union and Japan decide to create the world´s largest area of safe data flows*" press release, IP/18/4501, 17 July 2018, Tokyo

[188] Decision (EU) 2018/1907 — conclusion of the Agreement between the EU and Japan for an Economic Partnership, Official Journal L 330, 27.12.2018

[189] REINKE, op. cit. 6, p. 42

[190] COMMISSION IMPLEMENTING DECISION (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, Official Journal L 76/1

[191] Ibid

Interestingly, where the Commission's assessments reached a negative conclusion, as has happened twice in the past in relation to India, no recommendation is forwarded to the EDPB, which issues no opinion, and is little known about the reasons for the negative assessment. [192]

As the recent active adequacy decisions demonstrate, data protection is an important element intimately tied to trade negotiations and agreements.

2.1.2. Appropriate safeguards

Appropriate safeguards are one of the tools offered by the GDPR in the absence or instead of a positive adequacy decision when performing international personal data transfers outside the EU. Appropriate safeguards include[193]:

i) Legally binding and enforceable (contractual) instruments governing data transfers strictly between public authorities (Art 46(a) GDPR). Instruments must provide enforceable rights, legal remedies and claims for compensation (GDPR Recital 108).

ii) Legally Binding Corporate Rules (BCRs) governing transactions between the EU and overseas divisions of a corporate group (e.g. franchises, holding groups etc.) (Art 46(2)(b), 47 GDPR)

iii) Standard data protection clauses (or Standard Contractual Clauses (SCC)) adopted by the Commission (Art 46(2)(c) GDPR) or Member State´s Supervisory Authorities and approved by the Commission (Art 46(2)(d) GDPR

iv) Codes of Conduct (Art 46(2)(e), Art 40 GDPR)

v) Data Protection certification mechanisms, marks and seals (Art 46(2)(f), Art 42GDPR) (ICO website – "International Transfers")

Without either a positive adequacy decision or any of the safeguards mentioned above, data transfers can only take place if some derogation for specific situations as detailed in Art 49 GDPR applies.[194]

2.1.2.1. Standard Contractual Clauses (SCCs)

Standard contractual clauses (or standard data protection contractual clauses) may be used as an alternative method, in case of absence of a positive adequacy decision, for ensuring adequacy to allow a transfer to go forward.[195]

---

[192] GREENLEAF, Graham. *Questioning 'Adequacy'*. UNSW Law Research Paper No. 18-1. 2018

[193] These available instruments for data transfer from the EEA to the UK have also been confirmed by EDPB (12 February 2019) "*Information note on data transfers under the GDPR in the event of a no-Deal Brexit*", p. 2-4

[194] Art 49 GDPR

[195] Article 28 GDPR

Art 28 GDPR (Processor)(and Recital 81 of the GDPR) provides that where a data processor carries out any processing on behalf of a data controller, the controller must have a prior specific or general written authorization between the two parties. If the processor engages with sub-processors for processing activities, the same obligations as between the controller and the processor must apply (Art 28(4) GDPR). The data controller can enter into an individual contract (referred to as a "data processing agreement"(DPA), a "service contract" or a "data transfer agreement" for intra-company data transfers) or rely on standard contractual clauses (SCC or "model (contract) clause") which have been either adopted by the EC or by a Member State´s Supervisory Authority and approved by the Commission.[196]

This mechanism provides adequate data protection for international transfers. Art 28(3) stipulates the minimum requirements for SCCs, including two clauses:

i) The data processor "*processes the personal data only on documented instructions from the controller*," and

ii) The data processor must have "*sufficient guarantees to implement appropriate technical and organisational measures*"(Art 28(1) GDPR) to prevent unauthorised or unlawful processing of, and accidental loss or damage of personal data.

Article 28 allocates responsibility for publishing the SCCs to the EC (Art 28(7) GDPR) and to the Member State´s Supervisory Authority (Art 28(8) GDPR), which would be ICO in case of the UK.

The EC has adopted two sets of model clauses[197] for data transfers to "third countries"/non-EU countries, namely:

i) EU Controller to non-EU or EEA controller (Set I) (Commission decision 2001/497/EC), as amended by the EU Controller to non-EU controller or EEA Controller (Set II) (Commission decision 2004/915/EC)

ii) EU controller to non-EU or EEA processor (Set I) (Commission Decision 2010/87/ECC)

On 4 June 2021, the European Commission adopted the two sets of standard contractual clauses, as mentioned one for the use between controllers and processors within the European Economic Area (EEA, comprised of the 27 Member States of the EU as well as Iceland,

[196] Art 28 GDPR; REINKE, op. cit. 6, p. 42

[197] European Commission. *Standard Contractual Clauses (SCC) - Standard contractual clauses for data transfers between EU and non-EU countries*. European Commission [online]. European Commission, 2023, 1 [cit. 2023-10-20]. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Liechtenstein and Norway) and one for the transfer of personal data to countries outside of the EEA.[198]

Although the SCCs are a popular method used for intragroup transfers, as it merely requires adding data protection clauses to a single master contract. Nigel Parker from Allen and Overy notes a criticism marking it as "*depressing exercise that involves a lot of companies putting in place a lot of paperwork*" and that "*the contract changes do not improve citizen´s data protection, but merely fulfil a regulatory purpose*".[199]

Another big question is what happens if the UK develops later its own adequacy standards and shares data with countries that it, but not the EU, has determined to be adequate, such as China or India? The EU may not look too keenly at such evolvement, as data being transferred to these countries, such onward transfers must be insured by the UK as providing a level of protection equivalent to the EU´s and match the EU process and criteria in making its own adequacy decisions. This would form a key part of keeping the positive adequacy decision. [200]

The flow of data from non-EU countries into the UK is also regulated by foreign jurisdictions, allowing such transfers, which have their own rules on the transfer of data internationally. This means that the UK must keep in mind that its decision on whether to diverge from the EU standard can have an effect on its international trade relationships with other third countries, which in the case of the UK diverging from the EU data protection framework, may not deem the UK as a country with adequate level of personal data protection and would not want to transfer personal data there. That being said, the UK enjoys the following post-Brexit options concerning international personal data transfers[201], being:

i) To keep relying on the adequacy decision as if they were their own (ICO´s), utilising its mechanisms indefinitely and utilising the alternative mechanisms that GDPR has to offer (just as the EU does) in case of cessation of adequacy.

---

[198] European Commission. *New Standard Contractual Clauses - Questions and Answers overview - Frequently asked questions on the new SCCs*. European Commission [online]. European Commission, 2023, 1 [cit. 2023-10-20]. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en#:~:text=Standard%20contractual%20clauses%20%28SCCs%29%20are%C2%A0standardised%C2%A0and%C2%A0pre-approved%20model%20data%20protection,arrangements%20with%20other%20parties%2C%20for%20instance%20commercial%20partners

[199] TRENTMANN, Nina. *Companies Weigh Data-Privacy Risks Ahead of Brexit*. Wall Street Journal [online]. Wall Street Journal, 2019, 1 [cit. 2023-10-20]. Available at: https://www.wsj.com/articles/companies-weigh-data-privacy-risks-ahead-of-brexit-11552363260

[200] REINKE, op. cit. 6, p. 54

[201] Ibid

ii) To ignore the EU framework in the future (i.e. quit "transposing") EU adequacy decisions and rely on the UK´s own legal arrangements with non-EU countries, which may entail utilizing the GDPR alternative mechanisms much more extensively in order to maintain its own adequacy with the EU.

Maintaining compliance with the EU personal data protection framework as of now seems to be the easiest way to facilitate EU-UK personal data transfers as well as keeping international trade relationships that are dependent on international personal data transfers intact.

2.1.2.2. Newer GDPR mechanisms: approved Codes of Conduct and accredited third-party certifications

Codes of Conduct (Art. 40-41 GDPR) and certification procedures (Art. 42-43 GDPR) can also provide adequate measures for safeguarding data transfers. These measures can assist in meeting specific requirements in various sectors and can be particularly useful for micro-companies and SMEs. However, for these methods to be effective, the organizations in third countries must make binding and enforceable commitments to data subjects. The EDPB has produced specific guidelines on the proper accreditation of certain bodies (EDBP, 4 June 2019, Guidelines 4/2018)[202], on certification criteria (EDBP, 4 June 2019, Guidelines 1/2018)[203], on the adoption of Codes of Conduct, covering acceptance criteria for codes and requirements for issuing bodies (EDBP, 4 June 2019 - Guidelines 1/2019)[204]. Codes of conduct work on voluntary self-regulating basis and allow businesses to demonstrate industry-specific accountability to Member State´s Supervisory Authorities. They can be created through industry associations or trade bodies that represent controllers, but they must be monitored by independent accreditors and approved by the Supervisory Authorities or granted general validity by the EC.[205] Certifications are also on a voluntary basis and follow a similar accreditation process, however, they govern more specific processing activities and can be issued only to the data controllers or data processors in their scope.[206]

Codes of Conduct must be submitted for approval to the competent Supervisory Authority, which has to provide an opinion on whether it complies with the GDPR, then either approve or

[202] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)
[203] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation
[204] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679
[205] Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 Version 2.0
[206] Ibid

dismiss the draft Code od Conduct.[207] If a Code pertains to processing in multiple Member States, then the relevant Supervisory Authorities should request an opinion from the EDPB, to determine whether the draft Code provides sufficient safeguards. The Commission may then, after due examination, adopt the EDPB-recommended Codes for general use in the EU, and make them publicly available. A Code of Conduct-issuing body that is accredited by a Supervisory Authority is responsible for monitoring compliance with the Code of Conduct.[208]

In case of Transnational Codes of Conduct, the Commission must make the final decision. If the Commission´s decision overrides an ICO/Supervisory Authority decision, it may transgress the UK government´s "Brexit red lines", such as *"putting UK citizens first*"[209]. The same difficulties complicate the accreditation of monitoring bodies by the ICO. [210]

Data protection certification procedures and data protection seals and marks are voluntary schemes that demonstrate adequate safeguards in line with accountability principles set by the controller and processor. Additional binding and enforceable commitments through contractual or other legally binding instruments are expected.[211] The certification shall be issued by the competent Supervisory Authority or the EDPB, and shall last no more than three years, subject to periodic reviews and then come up for renewal. The EDPB shall maintain a public register of all certification mechanisms, seals, and marks. The EDPB may also adopt a common certification, or the "European Data Protection Seal".[212] As in the case of Codes of conduct, the Supervisory Authority must also accredit the independent certification bodies for the issuing, periodic review and withdrawal of certification. [213]

The ICO needs to collaborate closely with the EDPB by providing certification criteria and procedures, certifications and seals. Simultaneously, the Commission and EDPB should have complete trust in the ICO to establish appropriate technical standards for certification procedures, seals and marks in compliance with EU law. Article 55 (Competence) of the GDPR requires that the ICO must be "*competent for the performance of the tasks assigned to and exercise of the powers conferred on it in accordance with this Regulation*", however, this also means that the ICO must fully align to EU regulations and EDPB guidance. Naturally, the EU also has to endorse the ICO´s competence for the performance of these tasks, and to act as a lead national Supervisory

[207] Art 40(5) GDPR
[208] Art 40, 41(1) GDPR
[209] House of Commons Library (21 June 2017) "Brexit: red lines and principles", Briefing paper by Vaughne Miller, number 7938
[210] REINKE, op. cit. 6, p. 55
[211] Art 42(2) GDPR
[212] Art 42(5), 42(8) GDPR
[213] Art 43 GDPR

Authority, as well as to delegate to ICO authorisation and advisory powers under the GDPR and to trust its consistency (Art 63 (Consistency Mechanisms) GDPR).[214]

2.1.2.3. Other Safeguards - Binding Corporate Rules

Binding Corporate Rules (BCR) in accordance with Art 47 of the GDPR enable international organisations and groups of organisations to make intra-organisational personal data transfers. BCRs have to be approved by a BCR Lead Supervisory Authority, which must be in charge of coordinating them.[215]

The BCRs are not considered to be an ideal post-Brexit solution for international data transfers, for the following reasons[216]:

i) The lengthy application period is not intended for the mass market. The EU has a mutual recognition process where a Member State is the "Lead Authority", but a simple application can still take up to 12 months to complete. The EU has a mutual recognition process where a Member State is the "Lead Authority", but a simple application can still take up to 12 months to complete. Also, the uptake of the BCRs has been low (as of 2018 for example only 131 companies have obtained authorisations from the EU, including 27 BCRs from the UK´s ICO).[217]

ii) The Commission currently plays a crucial role in the BCR approval process. BCRs are not as inclusive as adequacy decisions and are disproportionately expensive for small and medium-sized enterprises (SMEs). Legal firms estimate an average setup cost of 250,000 GB pounds.[218]

2.1.2.4. Derogations for specific purposes

In the absence of an adequacy decision or appropriate safeguards, personal data may be transferred to a third country or international organization under the conditions outlined in Article 49 of the GDPR, i.e. on the basis of Derogations for specific purposes. It is essential to mention that Derogations for specific situations provide a legal basis for data transfers, that are supposed to be only occasional, not frequent, and should only affect a limited number of data subjects and be necessary to the data subject´s compelling legitimate interests without compromising their

[214] Art 55, 58(3); 63 GDPR, REINKE, op. cit. 6, p. 57
[215] Article 47 GDPR
[216] REINKE, op. cit. 6, p. 57
[217] Ibid
[218] Ibid

interests or their rights. Derogations for specific purposes can be summarised under the subsequent three categories[219]:

i) Explicit consent by the data subject, according to Article 49(1)(a) GDPR. This article establishes a legal basis for transferring data if "*the data subject has explicitly consented to the proposed transfer*" after being provided with all the relevant information about the risks associated with such transfer.

ii) Performance of a contract, according to Article 49(1)(b) GDPR). This article gives data controllers grounds for data transfers if "*the data subject has approved such transfer in advance*" and "*the transfer is necessary for the performance of a contract between the data subject and the "controller"* or "*the transfer is "necessary for the performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person*".

iii) Legitimate interest and other reasons, according to Article 49(1)(c-g) GDPR. This article also provides a legal basis for data transfers when "*the transfer is necessary for important reasons of public interest*", "*if it is necessary for the establishment, exercise or defence of legal claims*", if "*the transfer is necessary in order to protect vital interests of the data subjects (and) where the data subject is physically or legally incapable of giving consent*", or if "*the transfer is made from a register which according to the EU or Member State law is intended to provide information to the public and which is open to consultation*" under the strictures of EU law.

These alternatives for transfers to inappropriate countries and exemptions from the provisions of the GDPR are, however, more limited in scope than the adequacy decision, in particular the alternatives are examined in cooperation with Member States in the framework of the EDPB.[220]

2.2. Summary of the Chapter

To summarize the contents of this Chapter, international cooperation requires a mutually agreed framework and mechanisms, within which coordination for data transfers can take place. The GDPR offers multiple solutions for personal data transfers to third countries which were dissected in this Chapter.

The GDPR data transfers system operates on the default position that transfers of personal data to third countries should not take place unless a legal mechanism in Chapter V of the GDPR

[219] Article 49 GDPR
[220] Article 70 GDPR

allows the transfer of personal data to a third country. There are three legal mechanisms for data transfers. Adequacy decisions according to Article 45 GDPR; instruments providing appropriate safeguards in Article 46 GDPR; and derogations for specific situations in Article 49 GDPR.

The first legal mechanism is to achieve a positive adequacy decision, allowing the third country to transfer data to the EU/EEA/EFTA. Adequacy decisions are not infinite as they are periodically reviewed every four years. Their main advantage is that there is no additional effort required for businesses to transfer personal data and they aim to facilitate international data transfers so that third countries can act as a part of the Internal Market. The downside of adequacy decisions could be the fact that the adequacy decision can be obtained from the Commission and such process is not entirely transparent with political and economic factors coming into the picture. Another downside might be the fact that once a third country stops being compliant with the GDPR framework, the adequacy decision can be easily revoked. The UK achieved a positive Adequacy decision after post-Brexit negotiations which was the preferred outcome in the eyes of both UK and EU businesses.

If a third party does not achieve a positive adequacy decision, it has to rely on tools listed as the legal mechanisms called appropriate safeguards, including Standard Contractual Clauses, Binding Corporate Rules and Approved Codes of Conduct. Such tools are often paired with higher costs for businesses and more extensive paperwork to enable international data transfers. Standard Contractual Clauses are a possibility for the UK if their adequacy decision fails, as for example happened in the US after Schrems II revoked the Privacy Shield.

Another tool is Data protection certifications, marks and seals, which contain binding commitments to EU data subjects by third-country organisations and are mostly preferred in particular sectors having specific requirements and for the needs of micro-companies and SMEs.

Lastly, there is the possibility of using Derogations based on consent, contract performance or legitimate interest as described in Article of 49 GDPR. Derogations only have a limited scope in specified situations and are used on the basis of exceptional or occasional data transfers.

3. International data transfer legal framework in the UK

The UK economy is recognized as particularly data-driven and its success is dependent on untrammelled cross-border movement of data. However, the data transfers between the EU and the UK, post-Brexit, must be processed and transferred within the adequate legal framework decreed by the EU. The objective of any common legal framework must be clearly defined with the inclusion of regulatory cooperation that goes beyond mere recognition, which is provided in the Commission's adequacy decision.

3.1. The road to the UK Adequacy decision

In this section, the author would like to follow up on the previous Chapter addressing the important adequacy decisions, and include a wider historical background for the predispositions of the UK, for receiving a positive adequacy decision as such predispositions were heavily discussed during the Brexit negotiations. The subsequent sections will be more focused on dissecting the specific actions taken after the Brexit decision ensued as well as the outlook on the future of the UK´s Adequacy decision currently in place.

The UK Withdrawal Act enshrines the EU GDPR in UK statute law, so that its fundamental principles, the implications it imposes on business organisations, and the rights it accords to data subjects will continue to stand.[221] After Brexit the UK is still a member of ECHR. It is therefore under the jurisdiction of ECtHR, which has made some landmarks on the matter of privacy and data protection rulings such as the regulation of eavesdropping powers (*Case of Klass and Others v. Germany*)[222] and mass surveillance (*Big Brother Watch and others v. UK*)[223], interception of telephone conversations (*Malone v. United Kingdom*)[224] blanket mobile phone interception devices (*Case of Roman Zakharov v. Russia*)[225], excessive collection of medical data (*Case of L.H. v. Latvia*)[226].

---

[221] REINKE, op. cit. 6, p. 41-42
[222] KLASS AND OTHERS V FEDERAL REPUBLIC OF GERMANY, Judgment, Merits, App no 5029/71 (A/28), (1979-80) 2 EHRR
214, IHRL 19 (ECHR 1978), 6 September 1978, European Court of Human Rights [ECHR]
[223] Brother Watch and Others v. the United Kingdom, App no 58170/13, 62322/14 and 24960/15, ECHR 2018, GRAND CHAMBER 2021, 25 May 2021 European Court of Human Rights [ECHR]
[224] MALONE v. THE UNITED KINGDOM (Application no. 8691/79), JUDGMENT STRASBOURG 2 August 1984, European Court of Human Rights [ECHR]
[225] ROMAN ZAKHAROV v. RUSSIA, App no 47143/06, JUDGMENT STRASBOURG, 4 December 2015, European Court of Human Rights [ECHR]
[226] L.H. v. LATVIA (Application no. 52019/07) JUDGMENT STRASBOURG 29 April 2014 FINAL 29/07/2014, European Court of Human Rights [ECHR]

The aforementioned rulings of the ECtHR, however important they are, do not create a sufficient framework of data protection, as per the opinion of the Commission and its concerns about the privacy of the data being transferred from the EU to the UK, because of the conflict of law enforcement and surveillance practices in the UK. Moreover, the ECtHR does not specialise in data processing and data transfers in its great amplitude and therefore cannot maintain the ongoing equivalence of UK and EU data privacy and protection law by itself. Brexit supporters often spoke of taking back the law from the control of the EU, however, the pressure that applies to the UK after Brexit on keeping compliance with the data protection levels and to maintain or replace the ongoing trade deals may have been a double-edged sword.[227]

The UK has ratified the data protection framework by the Council of Europe´s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). As the EU Agency for Fundamental Rights has stated, "*The signatories of the EU Charter commit to respect the right to private and family life, which public authorities may not interfere with, except in the interests of national security, public safety or the economic well-being of the country or for the sake of protecting the public health and the rights and freedoms of others*". However, under Clause 5(4) of the "Great Repeal Bill" (EU Withdrawal Act 2018 or the Withdrawal Agreement 2018) the CFR (Charter) will not be retained in UK law after exit from the EU. [228]

Article 45 of the GDPR spells out the basic criteria for assessing the third country´s level of data protection and privacy regime when data is transferred from the EU to such country. Section (2)c) of Article 45 GDPR states one such criterion to be "*international commitments the third country or international organisation concerned has entered into or other obligations arising from legally binding conventions or instruments as well as its participation in multilateral or regional systems, in particular with relation to the protection of personal data*".[229]

The UK ratified the Convention 108+ in October 2018, which touches upon all of the principles of data protection and privacy embedded in the GDPR. This modernised Convention allows for its Convention Committee to evaluate the effectiveness of the measures it has taken in its law, defines new special categories of personal data that require appropriate legal safeguards in order to be processed, requires the notification of "data breaches which may seriously interfere

[227] REINKE, op. cit. 6, p. 44
[228] Ibid, p. 44-45
[229] Art 45 GDPR

with the rights and fundamental freedoms of data subjects" without delay to the competent Supervisory Authority and strengthens the individual rights of data subjects. [230]

This means that the Commission can use the Convention Committee to assess the quality and adequacy of UK data protection law independently. Greenleaf suggests that the revised Convention 108 would not offer the same level of protection as the GDPR. However, it does require the "*Convention parties to at least provide protection which the EU would consider "adequate" under the GDPR.*"[231] This is why the EU endorses Convention 108 and why the UK should continue to abide by it.[232]

Convention 108+ expands the list of "sensitive" personal data to include genetic and biometric data. The Convention also strengthens individual data rights by allowing the right to withhold consent, the right to be promptly informed of any privacy breaches, and the right to be excluded from decisions that are based solely on machine processing.[233]

Nevertheless, as the UK is now considered a third country it is crucial for both parties to maintain the special, both social and economic relationship between the EU and the UK as a former Member State. Now that the EU has approved adequacy decisions for the UK, most EEA processors will be able to send personal data back to UK controllers with no restrictions.[234]

3.1.1. Safeguarding the rights of Data Subjects

As aforementioned, the transposition of the GDPR into the UK law through the UK DPA 2018 (Data Protection Act 2018) had a significant impact on the safeguarding of the data subjects´ rights. In its Chapter 12, the UK DPA 2018 had shaped the legal basis for safeguarding the rights of EU and UK residents and citizens, covering the key provisions, including special personal data categories[235], the rights of data subjects[236], transfers of personal data to third countries[237], the data

[230] REINKE, op. cit. 6, p. 24
[231] GREENLEAF, Graham. *International Data Protection Agreements after the GDPR and Schrems, (2016) 139 Privacy Laws & Business International Report 12-15*. 1. Australia: UNS Law Research Paper No. 2016-29, 2016, p. 3
[232] REINKE, op. cit. 6, p. 25
[233] BAKER, Jennifer. *What does the newly signed 'Convention 108+' mean for UK adequacy*? IAPP (International Association of Privacy Professionals) [online]. IAPP (International Association of Privacy Professionals), 2018, 30. October 2018, 1 [cit. 2023-10-19]. Available at: https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/
[234] ICO. *Overview – Data Protection and the EU: What if we lose adequacy?* In: INFORMATION COMMISSIONER´S OFFICE - ICO. *Ico.org.uk* [online]. 2023, 2023-10-19 [cit. 2023-10-19]. Available at: https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/#lose-adequacy
[235] Art 10-11 of the UK DPA 2018
[236] Art 12-14, 43-54 and 92-100 of the UK DPA 2018
[237] Article 18 of the UK DPA 2018

protection principles[238], security of data processing[239], data breach notification[240], and transfer of personal data to third countries.[241] In addition, the UK DPA 2018 includes specific Codes of conduct for data sharing, direct marketing, age-appropriate design, and journalism.[242] The ICO has clearly stated, "*The GDPR will still apply to any organisations in Europe who send you data, so you may need to help them decide how to transfer personal data to the UK in line with the GDPR*" including the issue of consent. Moreover, "*companies will still need to be in compliance with the GDPR*" even in a no-deal scenario.[243] It has stated that it intends to continue to work closely with European Supervisory Authorities to safeguard personal data.

3.1.2. Adherence to rulings of the ECHR and CJEU

What matters is whether the UK, as a "third country", remains one of the 47 member states of the Council of Europe, along with all EU Member States (CoE – Chart of signatures and ratifications of Treaty 005), i.e. a signatory to the Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, ETS No 5 (ECHR), and therefore subject to the jurisdiction of the European Court of Human Rights, to which recourse can be made in the event of breaches of the Convention by member states. Yet, some UK politicians have suggested that the United Kingdom should withdraw from the ECHR because they believe that the jurisdiction of the ECtHR limits the sovereignty of the UK Parliament in a similar way to the CJEU.[244] In fact, PM May was planning to include quitting the ECHR in her 2020 electoral manifesto.[245]

There has also been a suggestion from PM Boris Johnson in 2022, about leaving the ECHR, due to a ruling by the ECtHR, ordering to stop deportation of migrants from UK to Rwanda (N.S.K. v. United Kingdom (app. no. 28774/22)). This proclamation had no real impact whatsoever, and the rest of the UK Government dismissed such a plan. Senior Conservative leaders, including a cabinet minister, have made declarations, that their party is likely to campaign to leave the ECHR at the next election if Rwanda flights continue to be blocked. As of right now, there are no viable

[238] Art 34-42 and 85-91 of the UK DPA 2018
[239] Art 66,107 of the UK DPA 2018
[240] Art 67-68, 108 of the UK DPA 2018
[241] Art 72-78, 109 of the UK DPA 2018
[242] Art 121-124 of the UK DPA 2018
[243] ICO. *Information rights at the end of the transition period Frequently Asked Questions*, In: INFORMATION COMMISSIONER´S OFFICE - ICO. *Ico.org.uk* [online]. 2023, 2023-10-19 [cit. 2023-11-19]. Available at: https://ico.org.uk/media/for-organisations/documents/2617966/information-rights-and-eot-faqs.pdf
[244] BOFFEY, Daniel. *Brussel seeks to tie UK to European human rights court after Brexit*, The Guardian, 18 June 2018, [online] [cit. 2023-11-03], Available at: https://www.theguardian.com/law/2018/jun/18/brussels-seeks-to-tie-uk-to-european-human-rights-court-after-brexit
[245] REINKE, op. cit. 6, p. 69

attempts of the UK Government to abandon the ECHR and The UK Government's official communicated position is that the UK will remain in the ECHR.[246]

The Commission believes that the UK should remain a party to the ECHR as it serves as a privacy safeguard. However, if the UK denounces the ECHR, as well as the ECtHR´s judgements, a "*guillotine clause*" is in need in any bespoke EU-UK security partnership agreement, which would also impact the adequacy of the UK´s data protection standards. This could result in the Commission's adequacy decision being withdrawn or declared invalid by the CJEU.[247] If in the future the UK should trigger such a guillotine clause, it would nullify the EU-UK security partnership and would potentially endanger the UK´s adequacy.

Likewise, it is important to mention, that the CJEU will always retain jurisdiction over companies controlling or processing personal data that are established in the EU, including the transfer of personal data in and out of the EU from and to the UK. This means that the UK cannot be used as a safe haven by US tech companies looking to evade the data protection regulations of the Council of Europe and the EU. The UK government should avoid flouting EU law, even after it is no longer under the jurisdiction of the CJEU. The EC and the CJEU, along with the ECtHR (if we leave it out of account), will still have a significant impact on data transfers to and from the UK, even without formal jurisdiction.[248]

3.2. Brexit from the perspective of EU data protection law

On 31 January 2020, the UK formally left the EU, after being a Member State of the Union for 47 years, following the outcome of the historic and unparalleled "*Brexit*" referendum, which took place on 23 June 2016, in which a participating majority of UK´s eligible voters chose to vote for "*Leaving*" the EU.[249] The decision to leave the EU, at the time the UK's largest trading partner and one of the world's largest trading blocks[250], was a significant historical decision, as it was the first country in the history of the Union to leave, and therefore an unprecedented example of what happens, when a Member State chooses to leave the Union.

---

[246] EARDLEY, Nick. *Tories could campaign to leave European human rights treaty if Rwanda flights blocked*, BBC News, 9 August 2023, [online] [cit. 2023-12-03], Available at: https://www.bbc.com/news/uk-politics-66438422

[247] European Commission, *Framework for the future relationship: Police and judicial cooperation in criminal matters*, Task force for the Preparation and Conduct of the Negotiations with the United Kingdom under Article 50 (TEUTF 50)

[248] REINKE, op. cit. 6, p. 70

[249] Brexit is a neologism of British and Exit coined in 2012 by Peter Wilding which expresses the UK's withdrawal from the EU; https://www.bbc.com/culture/article/20190314-how-brexit-changed-the-english-language, Accessed November 2023

[250] House of Commons Library, *Research Briefing: Statistics on UK-EU trade*, 10 November 2020, Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-7851/

Whereas Brexit was a historic milestone for the UK, it was expected of the UK´s government to have, at the bare minimum, engaged in contingency planning and preparations for the future trading relationship it would seek with the EU and other countries, before the referendum. Alas, such contingency planning and preparations did not really occur, partially, because it was not fully expected that the winning vote would be to "*leave*".[251]

Consequently what ensued, after the referendum´s outcome, was a great deal of political turmoil, including the resignation of two prime ministers and a request from the UK government to postpone the UK´s departure from the EU on three separate occasions in the next three years, following the discord amongst UK government ministers, over the scope and terms of the withdrawal agreement, before the EU and UK eventually agreed on the terms of a Trade and Cooperation Agreement (TCA). The Trade and Cooperation Agreement was concluded on 24 December 2020, only seven days before the UK would have "*crashed out*" of the EU on a "*no-deal*" Brexit.[252]

The discord among the UK Government and the previous failure to prepare for the post-Brexit period included no preparations on the scope of the data protection arrangements and measures. It was unclear, if the UK would even go on to comply with the EU data protection laws, most importantly the GDPR framework regarding the transfers of personal data between the EU or the EEA and the UK, and internationally as well. A significant question emerged: whether to diverge, either immediately or in the longer term, from the EU data protection law. The UK chose not to diverge, for now, which will be addressed later on in this chapter, when taking a closer look at the EU-UK adequacy decision.[253]

In the subsequent sections of this chapter, the author would like to go over what influenced the UK's decision on continued compliance with EU data protection standards after becoming a third country. The author would then like to comment on why the UK initially tried to pursue the exceptionalism strategy, seeking a bespoke data protection agreement outside the scope of the GDPR adequacy framework, before ultimately conceding on needing an adequacy decision from the EC to facilitate EEA-UK personal data transfers.

Although the UK adequacy decision currently demonstrates an adequate level of personal data protection between the EU and the UK, it may prove unstable later on. In this Chapter, the author would like to consider whether longer-term divergence is likely or not.

---

[251] DE HERT, Paul; GONZÁLEZ-FUSTER, Gloria and VAN BRAKEL, Rosamunde. *Research handbook on privacy and data protection law: values, norms and global politics*. Cheltenham, England: Edward Elgar Publishing, 2022. ISBN 1-78643-851-8, p.36

[252] Ibid

[253] Ibid, p.37

The EU data protection advocates have identified the UK's ongoing compliance with the GDPR as evidence of the EU's regulatory power and ability to "*export its laws and standards to third countries by offering unrestricted access to its large and valuable marketplace of personal data in return for confirmation of legal compliance, via an adequacy assessment*."[254]

Nevertheless, to make sure that the GDPR standards become and remain the global norm, it must ensure that it remains fit for purpose, hence why it can be put simply that the UK has left the EU but not the EU data protection law behind, for now, at least.[255]

3.2.1. The UK´s bargaining power to shape the EU-UK data protection relationship

The "*Exiting the EU*" Select Committee of the House of Commons published a report on Data flows and data protection after Brexit.[256] The report recognizes the Commission's authority to determine the adequacy of UK's data regime. It, however, proposes that a bilateral international agreement on data (i.e., a treaty) forms the basis of future relationships.[257]

During Brexit negotiations, Prime Minister May aimed for the UK's ICO to maintain its membership in EDPB and participate in the EU's "one-stop-shop" supervisory mechanism.PM May understood that the CJEU must continue to have jurisdiction over certain aspects of data protection after Brexit.[258] The EU, however, to guard its decision-making autonomy, has yet to allow any third party to sit in the EDPB, including even EEA countries like Norway.[259]

PM May proposed in her Florence[260] and Munich Speech[261], that close cooperation with the EU agencies in areas of security, criminal justice, and law enforcement should continue after Brexit. Based on the aforementioned, the future relationship between the UK, Europol, and Eurojust should include continued EU-wide data sharing and cooperation.

Upon analysing and reading between the lines of these two speeches, the UK was using its sophisticated intelligence and security capabilities as "*bargaining chips*". Although this thesis

---

[254] BENDIEK A. and RÖMER M. *Externalizing Europe: the global effects of European data protection,* 2019, Digital Policy, Regulation and Governance, ISSN 2398-5046, Emerald, Bingley, Vol. 21, p. 32-43, 33 and 35; MÜLLER Patrick and FALKNER Gerda, *The EU as a policy exporter? The conceptual framework*, in Gerda Falkner and Patrick Müller (eds), EU Policies in a Global Perspective: Shaping or Taking International Regimes?, London: Routledge, 2014, p. 11–12.

[255] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p.37

[256] House of Commons, Exiting the European Union Committee, 26 June 2018. *The progress of the UK´s negotiations on EU withdrawal: Data*, Seventh Report of Session 2017-19, HC 1317

[257] Ibid, para. 30

[258] Ibid, para. 31

[259] Ibid, para. 36

[260] Prime Minister Theresa May. *PM´s Florence Speech: a new era of cooperation and partnership between the UK and the EU*, speech transcript, (PM Theresa May, 22 September 2017)

[261] Prime Minister Theresa May. *PM´s speech at Munich Security Conference*, speech transcript (PM Theresa May, 17 February 2018)

focuses mostly on the legal aspects of personal data transfers, it is important to note that political power play was crucial with regard to the negotiations on the future EU-UK relationship and therefore on the future regime of the EU-UK personal data transfers. It is important to note that the May Government believed that Brexit negotiations were not just technical discussions between subject matter experts but rather political contests between players with conflicting motives. [262]

The UK vision of a future deep and special partnership was summarized by the UK negotiating team in three pillars: i) an economic partnership transcending a Free Trade Agreement, ii) a security partnership for law enforcement and criminal justice, iii) cross-cutting cooperative accords on matters such as data protection, science an innovation, etc.[263]

The author could only access publicly available resources, as sensitive negotiations involving national security take place behind closed doors and are classified. It may be inferred, however, that these are the UK´s most valuable bargaining chips, notwithstanding that there are no precedents for a "*special treatment*" of exiting EU Member States. Such "*bargaining chips*" were so valuable, that the UK might have been able to win a special relationship on data with the EU.[264]

The "*Exiting the European Union*" The Select Committee report acknowledges the challenges of negotiating an international data protection agreement while stressing its benefits for regulatory harmonisation and business certainty.[265] The alternatives analysed by the Committee are deemed to be "*unsatisfactory substitutes*" that burden businesses with unnecessary bureaucracy.[266] Therefore, to ensure continuity of data flows in both directions, it is highly desirable to have an agreement beyond adequacy decision. The reason is that if the UK wants to maintain adequacy with the EU, it needs to establish its own mechanisms for third countries outside the EU. This would require cooperation with the EDPB and the use of some alternative mechanisms contained in the GDPR.

The UK has rightfully pointed out that it "*is going beyond minimum EU requirements and will implement the GDPR and Law Enforcement Directive in full. The DPA 2018 will provide a comprehensive and robust regulatory framework, compatible with the European Convention on Human Rights and CoE Convention 108*".[267] The UK had already accepted Title 7 of the

[262] REINKE, op. cit. 6, p. 74
[263] HM Government. May 2018, *Framework for the UK-EU partnership – Data Protection*, presentation prepared by the UK negotiating team
[264] REINKE, op. cit. 6, p. 74
[265] House of Commons. Exiting the European Union Committee, 26 June 2018, *The progress of the UK´s negotiations on EU withdrawal: Data*, Seventh Report of Session 2017-19, HC 1317, para. 47
[266] Ibid, para. 57
[267] HM Government. May 2018, *Framework for the UK-EU partnership – Data Protection*, presentation prepared by the UK negotiating team, p. 11

Withdrawal Agreement[268], providing assurances for the future to protect personal data already located in the UK, and has given assurances that the risk of gaps in the legal provisions for data transfers post-Brexit will be eliminated.[269]

3.2.2. Personal data protection during the negotiation period

The UK enacted the Data Protection Act 2018 (UK DPA 2018) to repeal and replace the Data Protection Act 1998, as it was already known, that the GDPR would supersede Directive 95/46/EC and would become directly applicable in all EU member states and EEA countries, still including the UK, from 25 May 2018 until the end of the transition period on 31 December 2020.[270] If the UK had failed to comply with the GDPR, it would have led to a breach of the UK´s obligations as a Member State during that period (31 January 2020 – 31 December 2020) which cause a huge disruption in personal data flows, as the EC would likely prohibit transfers from EU Member States to the UK due to such breach.[271]

The UK DPA 2018 was enacted for two interrelated reasons, the first being its legal and economic necessity, and the second being the fact that the UK government had not planned for a "*leave*" vote and its consequences before the referendum, so an alternative solution was absent at the time. The UK therefore opted for the easiest solution, which was to maintain its compliance with the GDPR during the transition period, until all of its merits had been properly evaluated, as the GDPR was also seen as the data protection golden standard worldwide and would facilitate the continuance of the UK trade relationships during that period.[272]

A particular cause for maintaining compliance with the GDPR was also its extra-territorial application to UK data controllers, offering goods or services to individuals, and simultaneously monitoring the behaviour of individuals in EEA countries, therefore ongoing compliance was necessary for such purpose.[273] Non-compliance would only increase the burden of data controllers and increase the business cost for organisations. Hence, the Withdrawal Agreement specified that

---

[268] HM Government. DexEU, Department for Exiting the European Union, *EU Withdrawal Bill, Withdrawal Agreement*, 21 November 2018

[269] House of Commons. Exiting the European Union Select Committee, *The progress of the UK´s negotiations on EU withdrawal: Data*, Seventh Report of the Session 2017-19, report together with formal minutes relating to the report, HC 1317, 3 July 2018

[270] The period was referred to as the transition period in the Withdrawal Agreement and called the implementation period by the UK government. Art 288(2) TFEU*; An EEA Joint Committee Decision of 6 July 2018 incorporated the GDPR into the EEA Agreement, and it entered into force in all three EFTA-EEA States,* 20 July 2018; Decision of the EEA Joint Committee, No 154/2018, Official Journal No L 183/23, 19.7.2018

[271] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 38

[272] The UK DPA 2018 provides for two separate regimes for general processing: one for processing within the scope of the GDPR and a separate, equivalent regime for processing that falls outside the scope of the GDPR (the "*applied GDPR*").

[273] Article 3 GDPR

the GDPR would continue to apply (with the exception of Chapter VII – co-operation & consistency) in the UK during the transition period, concerning personal data being transferred between the EEA and the UK, and data being received from the UK, would not be treated any differently to data received from any Member State, though the UK had become a third country.[274]

Essentially the Withdrawal Agreement created something of a "*GDPR-envelope*" that pertained to personal data processed in the UK during the transition period. Personal Data would continue to be processed in the UK, reliant on those arrangements after the transition period ended, thereby ensuring that the personal data of individuals residing in EEA countries would not lose GDPR protection once the transition period ends if an adequacy decision was not in place by then.[275] This solution was welcomed by many data protection experts because "*it could only have the effect of making transfers easier*".[276] On the other hand, only a few experts reacted with concern to such a solution, even though it would allow the UK to temporarily avoid compliance with the Schrems criteria i.e., fundamental rights limitations on surveillance.[277]

Per Karen McCullagh opinion: „*Drafting and implementation of Chapter V compliance measures e.g., contractual arrangements would have been a costly, time-consuming, and onerous exercise that would have unfairly penalised small- and medium-sized enterprises, causing harm to both the EU and UK economies, which both parties were keen to avoid, particularly as an adequacy decision could well be in place before the other mechanisms were finalised. The pragmatic 'fudge' minimised economic harm by ensuring that EEA/EU-UK personal data transfers continued unimpeded during the transition period.*"[278]

In order to maintain a somewhat seamless degree of continuity, the Withdrawal Agreement provided that the CJEU would continue to have jurisdiction to rule on questions of interpretation raised by the UK courts in relation to data protection law and that the UK courts would respect and follow the decisions of the CJEU during the transitional period. Simultaneously "*UK-based data controllers and processors, including those from non-EEA countries e.g., the US that had established a base in the UK for the purpose of trading in the EU single market continued to benefit from the One-Stop-Shop (OSS) principle*." [279]

---

[274] Art 73 of the Withdrawal Agreement, 21 November 2018
[275] Art 71 (a) and (b) Withdrawal Agreement, 21 November 2018
[276] BAINES Jon, DE REYA Mischon. quoted in Sam Clark, *No SCCs needed for data controllers governed by GDPR, ICO lawyer suggests*, Global Data Review Blog 12 October 2018, [online] [cit. 2023-11-03], Available at: https://globaldatareview.com/article/no-sccs-needed-data-controllers-governed-gdpr-ico-lawyer-suggests
[277] CYBERMATRON. *Data protection in the EU-UK Withdrawal Agreement - Are we being framed?*, Cybermatron Blog, 15 November 2018, [online] [cit. 2023-11-18], Available at https://cybermatron.blogspot.com/2018/11/data-protection-in-eu-uk-withdrawal.html
[278] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 39
[279] Ibid

The ICO would go on as the UK's designated national supervisory authority and its lead supervisory authority for the coordination of measures and complaints relating to cross-border processing (e.g. complaints originating from a Member State), with the assistance of other data protection authorities in the Member States affected by the processing, and therefore minimising the administrative compliance burden. However, as Chapter VII of the GDPR did not apply under the terms of the Withdrawal Agreement, the ICO ceased to be a full voting member of the European Data Protection Board (EDPB) as of 31 January 2020. Instead, the ICO was merely granted "observer" status, allowing the it to attend EDPB meetings (by invitation), but not to vote during this period.[280]

3.2.3. The "Brussels effect"

As previously established, the UK did not immediately declare continuance with GDPR compliance and EU data protection laws, even though it would secure an equivalent level of personal data protection and increase the chances of securing a positive adequacy decision from the Commission. Exports of data-enabled services from the EU to the UK were worth approximately £42 billion (€47 billion), whilst exports from the UK to the EU were worth £85 billion (€96 billion) in 2018[281], which should indicate an interest in preserving such exports. However, the political calls for Brexit were influenced by the desire to diverge from the EU as well as seeing the GDPR standards as too high and thought that lower and less expensive standards would give the UK leverage when engaging in trade deals with other countries.[282] The author sees a clear conflict caused by contradictory political and economic interests of the UK at the time.

The impact of not adhering to the EU standards would have meant a big hit to the UK businesses. UK businesses representatives were particularly weary of the trade power of the EU. For example, Antony Walker of TechUK emphasised that "*we have to remember the size of the UK market versus the size of the European market"*[283]*,* by which he meant that "*we will have to do that very much in partnership with the European Union, rather than simply boldly striking out by ourselves and hoping others will follow*".[284]

---

[280] Article 70 and 128(5) of the Withdrawal Agreement, 21 November 2018
[281] Estimated by the UK government's Department for Digital, Culture, Media and Sport by applying the UN definition of digitally deliverable services (DDS) to the UK Office for National Statistics data, cited in DCMS, Explanatory Framework for Adequacy Discussions, Section A: Cover Note, 13 March 2020, p.1
[282] FEDERATION OF SMALL BUSINESSES. *Manifesto European Elections 2014*, February 2014; CASTRO Daniel, Brexit Allows UK to Unshackle Itself from EU's Cumbersome Data Protection Rules, Centre for Data Innovation, 20 July 2016, [online] [cit. 2023-11-18] Available at: https://datainnovation.org/2016/07/brexit-allows-uk-to-unshackle-itself-from-eus-cumbersome-data-protection-rules/
[283] Ibid, para 129
[284] Ibid

A business with a global footprint needs to have consistent practices across its businesses; if, for example, a global business based outside the EU takes GDPR as the norm for its business as a whole, it logically has no interest in deviating from GDPR - quite the opposite.[285] Consequently, trade and market forces were drivers of the UK's continued compliance with the EU data protection law, post-Brexit.

In conclusion, it was strongly advised by the Sub-committee against diverging from the GDPR in the business sector. This adds to the viewpoint that the EU is able to through its "*trade power*", to "*export*" its laws and standards to other countries by offering improved access to its large and valuable market in return for legal compliance.[286]

The UK's application for an adequacy decision makes an example of a situation where the context of the adequacy decision often coming from a place of asymmetrical negotiating powers in an existing trade relationship between the EU and a third country. The EU wields a significantly stronger economic power than most third countries, including the UK, and such dynamic allows the EU to *de facto* impose its legal framework onto a third country, which is often dependent upon maintaining strong economic ties with the EU.

The EU is considered to be a strong "*market actor*" which is driving the said export and externalisation of EU regulatory policies and EU data protection laws. Such effect is being labelled as the "*Brussels effect*"[287] when describing the EU's "*unilateral regulatory globalisation*" as the extension of EU regulatory norms and practices beyond the EU territory but outside the structures and institutions of hierarchical public rule-making.[288]

3.2.4. A Bespoke Data Agreement or a Mutual Adequacy Decision?

When reviewing its options, the Sub-Committee in charge of the post-Brexit data protection framework was considering whether post-transition EEA-UK data flows would be best facilitated by seeking either a partial adequacy decision or a whole country adequacy decision from the European Commission.[289] In addition, the Sub-Committee discussed alternative solutions

[285] House of Lords. European Union Committee, *Brexit: the EU data protection package*, 3rd Report of Session 2017–19 – published 18 July 2017 – HL Paper 7, para. 128
[286] BENDIEK A. and RÖMER M. *Externalizing Europe: the global effects of European data protection,* 2019, Digital Policy, Regulation and Governance, ISSN 2398-5046, Emerald, Bingley, Vol. 21, p. 32-43, 33 and 35; MÜLLER Patrick and FALKNER Gerda, *The EU as a policy exporter? The conceptual framework*, in Gerda Falkner and Patrick Müller (eds), EU Policies in a Global Perspective: Shaping or Taking International Regimes?, London: Routledge, 2014, p. 11–12
[287] BRADFORD Anu. *The Brussels Effect: How the European Union Rules the World*, (OUP, 2012), Oxford Academic, 19 Dec. 2019, ISBN 9780190088613, XIV
[288] Ibid, p. 3
[289] Art 45(3) and 93(2) GDPR

to requiring individual data controllers and processors to adopt their own compliance measures such as model clauses or binding corporate rules.

The UK-established data controllers preferred a comprehensive adequacy decision covering the entire country instead of individual sectors, while maintaining alignment with the EU data protection framework. The alternative solutions seemed much more burdensome requiring financial and administrative load, compared to an adequacy decision offering "*stability and certainty for businesses*". In particular, SME UK-based data controllers and processors could not easily absorb the legal costs associated with drafting and obtaining approval for model clauses or other legal mechanisms to carry out data transfers.[290]

Although the Sub-Committee rightly focused on economic considerations, the government had to consider political factors as well. It was necessary to maintain support for the trade negotiations from the government to ensure that Parliament would ratify any deal reached. This highlights the conflicting interests between political and economic considerations during the transition period. A separate Data Protection Agreement (or "Bespoke Data Agreement") with the EU was seen as an alternative to acquiring an adequacy decision, to further politically visualise the divergence from the EU´s data protection rules and to further promote the UK´s independence as a sovereign country. Brexit was powered by the peoples vote to diverge from the EU and was seen as "*freeing*" the UK from the EU laws, institutions as well as the data protection framework, which in the eyes of Brexit supporters were "*against British interests*"[291] and "*CJEU judgments on data protection issues hobble the growth of internet companies*"[292], could be seen as going against the wishes and interests of the UK people.

In this regard, an adequacy decision would be unacceptable because it would require the UK to accept the supervision of various EU authorities. For example, the Commission would have the possibility to revoke the adequacy decision and the national data protection authorities of the Member States would have the power to order the suspension of the flow of data to the UK. The UK would also have to accept the authority of the European Data Protection Board as a "rule taker", meaning that the UK would have to accept the EDPB's decision without representation on the Board. This would likely be quite uncomfortable for those who see Brexit as a complete divorce

[290] House of Lords. European Union Committee, *Brexit: the EU data protection package*, Paper 7, Chapter 3, paras 112–115.
[291] WHITE, Michael. *Why John Whittingdale is politically tone deaf and 30 years out of date*, The Guardian Blog, 9 March 2016, [online], [cit. 2023-11-18], Available at: https://www.theguardian.com/politics/blog/2016/mar/09/why-john-whittingdale-is-politically-tone-deaf-and-30-years-out-of-date
[292] GOVE, Michael. *Why I'm backing Brexit*, The Spectator, 20 February 2016, [online], [cit. 2023-11-18], Available at: https://www.spectator.co.uk/article/michael-gove-why-i-m-backing-brexit/,

from the EU institutions.[293] And if the UK did not accept any EDPB decision, it could potentially very easily lose its adequacy status.

The UK would also have to accept an indirect supervisory role for the EU Council and the EU Parliament, as these bodies can ask the EC at any time to amend or withdraw the adequacy decision, on the grounds that its adoption exceeds the implementing powers provided for in the General Data Protection Regulation.[294] Furthermore, given that the EU is an autonomous legal order, any proportionality decision by the Commission between the EU and the UK could be challenged before the CJEU, which acts as the guardian of fundamental rights. Adopting such a supervisory role would represent a major concession by the UK government, which in its early statements on the UK's withdrawal from the EU described the end of the CJEU's jurisdiction as a "*red line*".[295]

As aforementioned, the initial pursuit of the UK government was to go with the strategy of exceptionalism. This meant proposing that the UK should receive preferential treatment in the form of a free trade agreement with the EU and close cooperation, inter alia, law enforcement and criminal justice, security and defence, and mutual recognition of data protection laws, subject to an adequacy assessment.[296]

The UK then further suggested that data protection disputes should be resolved through the provisions of the Trade and Cooperation Agreement, if concluded, rather than through the GDPR's supervisory and enforcement mechanisms. The underlying motivation was to prevent the EU from having the power to unilaterally revoke an adequacy decision and thereby immediately stop data transfers between the EU and the UK if the UK was found to be in material breach of the GDPR.[297]

---

[293] MURRAY, Andrew. *Data transfers between the EU and UK post Brexit?*, International Data Privacy Law, Volume 7, Issue 3, 2017, p. 151

[294] European Commission, *How the EU determines if a non-EU country has an adequate level of data protection*, [online], [cit. 2023-11-18], Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[295] KUNER, Christopher. *A Court of Justice International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15*, EU-Canada PNR, 2018, CML Rev, 55(3) 857–882; TAMBOU Olivia. *Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights,* (2018) European Foreign Affairs Review, 23 (2), 187–202; PAPAKONSTANTINOU, Vagelis and DE HERT, Paul. *The PNR Agreement And Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework On Either Side Of The Atlantic* (2009) CML Rev, 46(3) 885–919, EUROPEAN PARLIAMENT. *LIBE Committee, Briefing: Personal data protection achievements during the legislative term 2014–2019: the role of the European Parliament*, April 2019, [online] [cit. 2023-11-22], Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/608870/IPOL_BRI(2019)608870_EN.pdf

[296] DexEU. *The exchange and protection of personal data - a future partnership paper*, 24 August 2017[online] [cit. 2023-11-22], Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

[297] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 44

The EU did not accept the UK's exceptionalism approach, for a number of reasons. In particular, because the completion of the Single Market was achieved not only by removing barriers to the movement of capital, goods, services and labour, but also by creating a legal order and a corresponding set of measures to regulate economic activity within and across borders, including the GDPR, which governs data protection in all Member States.[298]

If the Commission were to unilaterally agree to a bespoke data agreement with weaker obligations, it could give a competitive commercial advantage to a third country and ultimately undermine the Single Market in its existence. Therefore, while the Commission has proposed "*non-negotiable horizontal provisions on cross-border data flows and protection*" to be included in trade agreements to reduce trade barriers such as forced national data localisation, it envisages their use only in situations where no realistic adequacy determination can be made in data protection monitoring.[299] It instead advocates that trade negotiations and adequacy requests be separate but parallel.[300]

This approach allowed the EU to achieve its goal of promoting the GDPR as a global standard while ensuring that its integrity and competitiveness are not undermined. Unsurprisingly, Michel Barnier, the EU's chief negotiator at the time, rejected the UK's proposal to regulate data protection on an individual basis, arguing that: "*The transfer of personal data to the UK will only be possible if the UK provides adequate safeguards. One example to ensure that adequate safeguards are in place is an 'EU adequacy decision'. This is an autonomous EU decision. There can be no system of "mutual recognition" of standards when it comes to the exchange and protection of such data*."[301] Barnier´s comments on the system of mutual recognition pre-date the EU-Japan mutual adequacy agreement mentioned in the previous chapter. They must be viewed and understood from the perspective of the UK's proposal for a bespoke adequacy agreement outside the scope of the GDPR adequacy criteria and procedure and his point about an adequacy decision being an autonomous decision made by the EC remains valid.

The UK Government subsequently proposed a new EU-UK agreement that would "*build on the standard adequacy agreement*" and acknowledged that the Commission would "*carry out*

---

[298] DexEU. *The exchange and protection of personal data - a future partnership paper*, 24 August 2017, [online] [cit. 2023-11-18], Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

[299] EUROPEAN COMMISSION. *Letter on cross-border data flows and EU trade agreements*, 1 Mar. 2018, [online] [cit. 2023-11-18], Available at: http://data.consilium.europa.eu/doc/document/ST-6687-2018-INIT/en/pdf

[300] EUROPEAN COMMISSION. *EU horizontal provisions on Cross-border data flows and protection of personal data and privacy in the Digital Trade Title of EU trade agreeme*nts, [online] [cit. 2023-11-18], Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_1462

[301] EUROPEAN COMMISSION. *Speech by Michel Barnier at Business Europe Day 2018, Brussels*, 1 March 2018, [online] [cit. 2023-11-18] Available at: http://europa.eu/rapid/press-release_SPEECH-18-1462_en.html,p. 8

an assessment to make sure we meet the basic equivalence test set out in the GDPR"[302], but neglected to specify how any disputes would be resolved. To no surprise, it was once again rejected with Barnier´s statement "*Who would launch an infringement against the United Kingdom in the case of misapplication of GDPR? Who would ensure that the United Kingdom would update its data legislation every time the EU updates GDPR? How can we ensure the uniform interpretation of the rules on data protection on both sides of the Channel?*" He concluded, that the UK has to come to an understanding that the only possibility for the EU to protect personal data is through an adequacy decision.[303]

Barnier insisted that the UK would have to agree to submit to an adequacy assessment and could not diverge from the EU's GDPR rules for a post-Brexit data protection agreement. As with any other country seeking a positive adequacy decision from the Commission, the UK would need to agree to periodic review of such decision and oversight by the CJEU. [304]

Following these exchanges, in June 2018 the UK government published a Technical Note on the benefits of a new data protection agreement which repeated the case for a bespoke legally binding agreement on the basis that: "*a key benefit of such an agreement, over a standard Adequacy Decision, is that we can negotiate the right governance mechanisms for our future data relationship. This could include an agreed approach to the standards applied and their interpretation, and to enforcement and dispute resolution*."[305]

The note summarized the advantages of a new EU-UK data protection agreement. It includes legal certainty, cooperation on enforcement and investigations, as well as efficiency savings for businesses and regulators working with the EU. This three-page "*vision*" foreran a more detailed white paper on "*the exchange and protection of personal data – a future partnership paper*", which stresses the benefits of the UK´s intent to build a "*new, deep and special partnership with the EU*". It noted that the UK starts from an unprecedented point of alignment with the EU, as a former Member State, and adoption of international data protection standards and proposes a UK-EU model for exchanging and protecting personal data and for regulatory cooperation.[306]

---

[302] HM GOVERNMENT. *Framework for the UK-EU partnership Data protection*, 25 May 2018,p. 16–17

[303] EUROPEAN COMMISSION. Speech by Michel Barnier at the 28th Congress of the International Federation for European Law (FIDE), Lisbon, 26 May 2018, SPEECH/18/3962, [online] [cit. 2023-11-18], Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_3962

[304] Ibid

[305] HM Government. Technical Note: Benefits Of A New Data Protection Agreement, 7 June 2018, [online] [cit. 2023-11-18], Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714677/Data_Protection_Technical_Note.pdf

[306] HM GOVERNMENT, Department for Exiting the European Union. *The Exchange and protection of personal data: A future partnership paper*, 24 August 2018, para. 26

Subsequently, the UK Government published another document reiterating its proposals but adding that "*the UK is prepared to enter into preliminary discussions on an adequacy assessment with a view to concluding a data protection agreement by the end of the implementation period at the latest*".[307]

The Commission´s negative standpoint on the bespoke data protection agreement outside the scope of the GDPR adequacy criteria and procedure led to a different proposal. The more pragmatic solution, by the UK's Exiting the EU Committee, recommended that the UK begin the process of applying for an adequacy decision without delay while continuing to explore the possibility of a bespoke agreement that could ultimately replace an adequacy decision.[308]

Given the economic need for the adequacy of the UK´s data protection framework, the UK pursued this course of action and made a political declaration outlining the intention to seek an adequacy decision from the EC. The EU agreed to make an adequacy assessment during the UK´s transition period "*if the applicable conditions are met*"[309] meaning that the UK should satisfy the 'essentially equivalent' level of protection test. The Commission had taken the view that the UK should be kept separate 'to keep trade deals uncontroversial',[310] particularly as "*For the EU, privacy is not a commodity to be traded. Data protection is a fundamental right in the EU*"[311] and protection of fundamental rights is non-negotiable.[312]

It is vital for the EU and UK trade relations to maintain the level of trust provided by the fact that the UK was a long-term Member State and implemented existing pre-Brexit EU data protection laws. Such trust does not automatically exist in relation to third countries, rather it must be built through formal legal relationships and as Lynskey notes "*it is this change in status i.e., from trusted member state to third country that explains why 'on the eve of the end of the transition period the UK is de facto "adequate" as an EU Member State while the following day it is not*".[313]

The UK however, as a sovereign state, is equally entitled to assess the adequacy of protection provided by EU member states and any other country seeking to engage in data transfers

---

[307] HM Government response to the Committee on Exiting the European Union Seventh Report of Session 2017–18, *The Progress of the UK's negotiations on EU withdrawal: Data* (HC 1317, 6 Sept. 2018), [online] [cit. 2023-11-18] Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmexeu/1564/156402.htm, para 3.
[308] Ibid, para 9.
[309] EUROPEAN COMMISSION. *Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom*, 2019/C 384 I/02, Official Journal 2019 C 384 I/02
[310] HANKE VELA, Jakob, PLUCINSKA, Joanna and VON DER BURCHARD, Hans. *EU trade, the Martin Selmayr Way*, Politico, 21 Feb. 201
[311] Ibid
[312] FONTANELLA-KHAN, James. *Data protection ruled out of EU-US trade talks*, Financial Times, 4 November 2013
[313] LYNSKEY, Orla. *Extraterritorial Impact in Data Protection Law through an EU Law Lens*, DCU Brexit Institute Working Paper Series – No 8/2020, p. 12

with it. Though the adequacy decision facilitates its trade relationships, it is the UK´s sovereign right to question the adequacy setting or try to replace it with alternative solutions.

3.3. The Trade and Cooperation Agreement

The Trade and Cooperation Agreement (the "TCA") was concluded on Christmas Eve 2020, after ten rounds of negotiations during an eight-month period, the UK and EU agreed upon the terms. The TCA has been applied on a provisional basis from 1st January 2021, pending approval, on the EU side, by the Council of the EU and the EU Parliament.[314]

The TCA was signed by both parties on 30 December 2020, when the UK Parliament approved it and it was implemented into UK law by the enactment of the European Union (Future Relationship) Act 2020. The TCA entered into force on 1 May 2021 after its ratification, by the Council of the EU and the EU Parliament on the basis of Article 217 TFEU.[315]

The scope of TCA was not as wide-ranging as many had hoped. However, it provided a level of certainty for avoiding tariffs or quotas on goods passing between the UK and the EU. The TCA allows for some mutual market access in services, but this is subject to further negotiations on certain aspects such as equivalence for financial services. It also includes cooperation mechanisms in various policy areas, including data protection and provides transitional provisions regarding EU access to UK fisheries and UK participation in some EU programmes.[316]

Title III of the TCA sets out the basis for the EU and the UK to cooperate on digital trade, i.e., trade carried out by "*electronic means*".[317] It is based on a reaffirmation of respect for the Universal Declaration of Human Rights and other international human rights treaties, by each of the parties.[318]

The TCA explicitly affirms each Party's commitment to a high level of data protection, as well as its commitment to work together to promote high international standards and engage in dialogue, exchange of expertise and law enforcement cooperation.[319] The agreement also states that both the UK and the EU agree not to restrict cross-border data flows. There is a list of the types of provisions that would be considered restrictions, ranging from data localisation provisions to requirements to use locally certified or approved computing facilities.[320]

---

[314] CELESTE Edoardo. *Cross-border data protection after Brexit*, DCU Brexit Institute Working Paper Series, No 4/2021, p. 7
[315] Ibid, p. 6
[316] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 46
[317] Art DIGIT.2, TCA.
[318] Art COMPROV.4, TCA
[319] Art COMPROV.19, TCA
[320] The provision is to be reviewed in three years; Art 6, TCA.

One criticised element of the TCA is that the Commission did not accurately include the EU's horizontal provisions on cross-border data flows and the protection of personal data and privacy, in the Digital Trade Title of the EU trade agreements, approved by the European Commission in 2018.[321] The relevant clauses do not state that data protection is a fundamental right and, as such, it may not receive the same level of protection as other fundamental rights. The second clause of the agreement contains language that may cause a conflict, if the privacy and data protection laws of the EU are contested during a trade dispute. In such a scenario, the EU would need to justify its data protection and privacy legislation based on the strict criteria outlined in Article XIV of the General Agreement on Trade in Services.[322]

Although the Commission's measures to "*soften*" the horizontal provisions were useful when the UK began trade negotiations with the EU, and are no longer relevant now that the UK has obtained an adequacy decision and the transfer of data falls within the scope of the GDPR, the Commission's approach could prove short-sighted if other third countries, such as Australia, that are conducting trade negotiations with the EU seek to negotiate the inclusion of similarly broad horizontal provisions in any trade agreement with the EU.[323]

The repeated inclusion of such clauses in trade negotiations could lead to a "*weakening*" of the EU's high data protection standards over time unless the third country requests an adequacy assessment by the EU. Unsurprisingly, the EDPS has expressed regret and concern that 'by changing the legal wording of the horizontal provisions, the FTA creates unnecessary legal uncertainty as to the Union's position on data protection in the context of EU trade agreements and risks creating friction with the EU data protection legal framework'.[324]

In an attempt to calm the situation and reaffirm the EU's commitment to high standards of data protection, the EDPS called on the Commission to "*clearly reiterate its commitment to horizontal provisions as the sole basis for future EU trade agreements with other third countries and [confirm] that data protection and privacy rights will not be a subject of negotiations*".[325]

---

[321] EUROPEAN COMMISSION. *Horizontal Provisions on Cross-border Data Flows and Personal Data Protection*, news release of 18 May 2018, [online] [cit. 2023-11-18]. Available at: https://ec.europa.eu/newsroom/just/items/627665

[322] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 47

[323] EDPS. *EDPS Opinion on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement, Opinion 3/2021*, 22 February 2021, [online] [cit. 2023-11-18] Available at: https://edps.europa.eu/system/files/2021-02/2021_02_22_opinion_eu_uk_tca_en.pdf, p. 8

[324] Ibid

[325] Ibid, p.10–11

3.4. TCA Transitional Data Protection Arrangements

The TCA itself does not include an adequacy decision to facilitate EEU-UK personal data transfers. Therefore, a Declaration attached to the TCA recorded the European Commission's intention to "*promptly launch the procedure for the adoption of adequacy decisions with respect to the UK under the General Data Protection Regulation*", once the adequacy assessment process was complete.[326] The TCA does not address adequacy as it is a separate process. The Commission had agreed to start its evaluation of the UK's adequacy, using the powers granted by Article 45(3) of the GDPR, simultaneously with the trade negotiations. However, the evaluation was not finished by the time the negotiations came to an end.[327] To avoid a data protection "*cliff-edge*" the TCA contained further transitional arrangements to facilitate EEA-UK transfers pending the outcome of the adequacy assessment. According to the aforementioned, the United Kingdom would not be considered a third country for the purpose of GDPR until a specified period ends. This period began on 1st January 2021 and would end either when an adequacy decision is made by the European Commission under Article 45(3) of GDPR or after four months, that is, until 1st May 2021. In case extra time is required for the assessment, the period could be, upon further agreement, extended by two months, i.e., until 1st July 2021.[328]

The UK's transition period was subject to certain conditions. One such condition was that the UK was not allowed to make any changes to its data protection legislation or exercise any "*designated powers*" during the specified period. This included recognizing other third countries as adequate for data transfer purposes, approving new codes of conduct, certification mechanisms, binding corporate rules, standard contractual clauses, or administrative arrangements. Making any such changes could jeopardize a finding of adequacy.[329]

The only changes allowed were to align with EU rules, like recognizing new Standard Contractual Clauses (SCC) adopted by the EU.[330] If the UK were to make any changes to its data protection laws or exercise any of the designated powers without consent, the bridging mechanism and specified period would automatically come to an end. [331]

---

[326] *Declaration on The Adoption of Adequacy Decisions with Respect to The United Kingdom*, Official Journal of the European Union L 444/1475, 31.12.2020.
[327] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 48
[328] Art FINPROV.10A (1) and (2), TCA.
[329] Art FINPROV.10A (3), TCA; DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 49
[330] EUROPEAN COMMISSION. *Data Protection -Standard Contractual Clauses for Transferring Personal Data to Non-EU Countries (Implementing Act)*, (Have your say), [online] [cit. 2023-11-18], Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries
[331] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 49

3.5. The UK Adequacy post-transition

As aforementioned, upon concluding the TCA, the UK's application for adequacy assessment was still underway as a separate, parallel process. The UK government was required to demonstrate to the Commission that the UK provides an adequate i.e., essentially equivalent level of protection to that in the EU by meeting the criteria in Article 45 of the GDPR and elaborated on in the EDPB's "*adequacy referential*," [332] and corresponding CJEU case law.[333]

The UK is now considered adequate under the GDPR and the Commission Implementing Decision 2021/1773 of 28 June 2021 on the adequate protection of personal data by the United Kingdom.[334] When the transition period ended, the GDPR was incorporated into UK law by virtue of regulations made pursuant to the European Union (Withdrawal) Act 2018. The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (DPPEC Regulations) renamed the GDPR as the "EU GDPR" and generated a "UK GDPR" by making numerous changes to the GDPR text to allow it to be retained as UK domestic law.[335]

For instance, references to EU institutions and procedures were understandably removed and replaced with appropriate post-transition terms e.g., references to "*Union or Member State law*" were replaced with references to "*domestic law*", and references to decisions made by the EU Commission were replaced with references to decisions made by the UK government. The UK DPA 2018 was similarly revised.[336] The principles, obligations, and rights for data controllers and processors and individuals remain unchanged.

As for transfers of personal data outside of the UK, they are only allowed if an adequacy decision or appropriate safeguard is in place or if a derogation applies. The DPPEC Regulations state that exceptions are still allowed, and all Binding Corporate Rules (BCRs) that have been authorized, as well as EU Standard Contractual Clauses that were issued by the EU before the end of the transition period, will continue to be recognized as valid by the UK. However, any new SCCs need to be submitted to the ICO or respective EU Supervisory Authorities. Likewise, a BCR

---

[332] Article 29 Working Party, *Adequacy Referential (2018)*, wp254rev.01, [online] [cit. 2023-11-23], Available at: https://ec.europa.eu/newsroom/article29/items/614108

[333] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 53

[334] EUROPEAN COMMISSION. *Commission Implementing Decision (EU) 2021/1773of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*, notified under document C(2021) 4801, Official Journal of the European Union L 360/69

[335] Statutory Instruments 2019 No. 419, Exiting the European Union Data Protection Electronic Communications, The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, 28 February 2019

[336] Ibid., Schedule 2.; Withdrawal Agreement, Art 128(5)

holder is required to transfer to the appropriate lead authority and appoint a representative, in the relevant jurisdictions.[337]

The UK preserved all EU adequacy decisions to ensure data flows (e.g., with respect to Andorra, Japan, Canada, and New Zealand), and by specifying that all EEA countries, EU institutions and bodies are considered to provide an adequate level of protection on a transitional basis. Gibraltar has been recognized as providing adequate protection as it is a British overseas territory.[338]

These steps have provided clarity and consistency for data flows in the short term. However, acknowledging the UK's regained regulatory autonomy, the UK Secretary of State for Digital, Culture, Media and Sport (DCMS) has been granted the power to conduct its own assessments of adequacy for transfers outside the UK.[339] There is very little information on the UK's criteria for assessing adequacy, except for their public statements that they plan to use an outcomes-based risk assessment approach. This is in the hope that they will be able to conclude the assessments more quickly than those conducted by the EU.[340]

It is understood that the adequacy assessment will consist of four distinct phases., the first being: i) gatekeeping, a process by which a specific team within DCMS will consider whether to commence an assessment of a third country (territory or sector) or international organisation for adequacy purposes. Second phase will consist of ii) an assessment,[341] that is, the programme of work associated with collecting and analysing information relating to the level of data protection in another country. Third phase will be iii) a recommendation to the secretary of state, and finally last, iv) a procedural phase, during which an adequacy regulation (the UK equivalent of an adequacy decision) will be drafted and laid before the Westminster parliament.[342]

The ICO and the DCMS are expected to meet at various intervals during the assessment process. The Secretary of State is responsible for issuing adequacy regulations, but they must consult with the ICO and other relevant parties. However, the Secretary of State is not bound by the views of the ICO and has the ultimate responsibility for issuing adequacy regulations.[343]

The government's Secretary of State will keep a record of countries, territories, sectors, and organizations that are considered to provide adequate data protection. If the Secretary of State

---

[337] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p.50
[338] Ibid
[339] Section 17A, UK DPA 2018
[340] *Statement made by Oliver Patel, Head of Inbound Data Flows, Department for Digital, Culture, Media and Sport (DCMS) at Commercial data transfers between the UK and EU and the adequacy decision*, Cross DPN Online Workshop, 22 April 2021
[341] Art 45 UK GDPR
[342] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p.50
[343] Section 182(2) of the UK DPA 2018; Art 36(4) of the UK GDPR

determines that a particular country doesn't provide adequate protection, then data transfers may be limited or restricted. This could happen if the Secretary of State refuses to create an adequacy regulation for that country or revokes an existing adequacy regulation if one already exists.[344]

3.5.1. Exemptions from the GDPR: Access to the personal data of EU citizens

The UK DPA 2018, Schedule 2 (Exemptions from the GDPR) Part 1(4) (Immigration) exempts the UK Government from conceding to individual rights requests "that would undermine the maintenance of effective immigration control". Leigh Day, the law firm that represents *the3million*, a non-profit organisation which is acting on behalf of EU citizens in the UK, argues that the Home Office post-Brexit could deny EU citizens access to their personal records when applying for "settled" status. The court heard that the Windrush immigration scandal showed that data were often inaccurate, and the Joint Council for the Welfare of Immigrants, the Law Society, and the Bar Council opposed such exemption in the UK DPA 2018. (Schedule 2 (Exemptions from the GDPR), Paragraph 4) introduced in the Home Office. This is also the view of the House of Commons Home Affairs Committee, which was unconvinced that all those involved in the Brexit negotiations fully understand the implications of access to data (Paragraph 6), and which also suggested that the immigration exemption in the UK DPA 2018 "could undermine a data adequacy decision".[345]

Barring access to one owns personal records kept by public bodies would also violate the EU Charter of Fundamental Rights, particularly Article 8 of which grants the data subjects the right to access to the data that has been collected about them, plus the right of the data subject to require any errors herein to be rectified. [346]

3.6. An "Unstable" Adequacy Decision

The Commission had to assess whether the UK's legislative framework for data protection was appropriate. However, it also had to make a judgment on the UK's political structures and values. This included assessing the country's respect for the rule of law, as well as human rights and fundamental freedoms.[347]

---

[344] DCMS. *Memorandum of Understanding on the role of The ICO in relation to New UK Adequacy Assessments*, 19 March 2021, [online] [cit. 2023-11-18], Available at: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments; DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p.50

[345] RIENKE, op. cit. 6, p. 67

[346] Ibid

[347] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 51

As part of the process, there was a need to evaluate the UK's data protection laws and exceptions to them, examine data protection methods and protocols, and scrutinize the supervisory capabilities in the Investigatory Powers Act 2016 concerning surveillance powers. Also, there was a need to review the provisions that permit the transfer of data from the EEA to third countries through the UK. To this end, the UK government submitted to the Commission a series of policy documents entitled the "*Explanatory Framework for Adequacy Discussions*",[348] covering a wide scope of topics, including the legislative framework, restrictions and processing conditions, and the role and effectiveness of the ICO, in which it set out its case for a finding of adequacy.[349]

Several shortcomings in UK laws and practices were identified that could pose a barrier to acquiring adequacy. This included the aforementioned overly broad immigration exemption in the UK's Data Protection Act 2018 and the UK government's decision not to retain the EU Charter in UK law. Declarations of an intention to "opt-out" of parts of the ECHR, or at least from interpretations of the Convention by the European Court of Human Rights,[350] raised further concern. The Investigatory Powers Act 2016 also lacked sufficient limits and safeguards on access to bulk data for national security purposes to comply with EU fundamental rights law.[351] Relatedly, the UK's membership in the Five Eyes Intelligence Sharing Alliance presented challenges related to transferring data from EEA countries to the US or other third countries without an adequacy decision.[352]

Given these deficiencies, the Commission's announcement on 19 February 2021 that it had completed its assessment and publication of a draft adequacy decision in which it found that the UK provides an adequate level of protection[353] was met with consternation in some circles. In particular, among those who had urged the Commission to adopt a fully strict interpretation of legal provisions and standards.[354]

---

[348] HM Government. *Explanatory framework for adequacy discussions*, 13 March 2020), [online] [cit. 2023-11-18] Available at: https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions

[349] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 51

[350] BOWCOTT, Owen. *UK government plans to remove key human rights protections*, The Guardian, 13 September 2020, [online] [cit. 2023-11-23], Available at: https://www.theguardian.com/law/2020/sep/13/uk-government-plans-to-remove-key-human-rights-protections

[351] BROWN Ian and KORFF Douwe. *The inadequacy of UK data protection law Part One: General inadequacy*, [online] [cit. 2023-11-23], Available at: https://www.ianbrown.tech/wp-content/uploads/2020/10/Korff-and-Brown-UK-adequacy.pdf, Case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, ECLI:EU:C:2020:790

[352] BROWN Ian and KORFF Douwe. *The inadequacy of UK data protection law Part One: General inadequacy*, [online] [cit. 2023-11-23], Available at: https://www.ianbrown.tech/wp-content/uploads/2020/10/Korff-and-Brown-UK-adequacy.pdf; DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 51

[353] EUROPEAN COMMISSION. *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, 13 April 2021

[354] DOUWE Korff. *The inadequacy of the EU Commission's Draft GDPR Adequacy Decision on the*

Following the Commission's announcement, the EDPB was also asked to conduct its own assessment and to provide its opinion on the UK adequacy decision. The EDPB observed a "*strong alignment*" on key areas between the EU and UK data protection frameworks on core provisions, such as lawful and fair processing for legitimate purposes, purpose limitation, special categories of data, and automated decision-making and profiling. It also pointed out the UK's formerly stated intention to diverge from the GDPR, and therefore welcomed the Commission's periodic recurring assessment of the adequacy decision each four years. Regarding surveillance powers and oversight, the EDPB opinion welcomed the establishment of the UK's Investigatory Powers Tribunal and its ability to review access to data by national security agencies. It also appreciated the establishment of the Judicial Commissioners in the Investigatory Powers Act 2016 to ensure better oversight, and to provide individuals with opportunities to seek redress. Despite the overall positive tone of the EDPB's opinion, there were several concerns that needed to be addressed. That included issues related to national security monitoring, bulk interceptions, independent oversight of automated processing tools, and the lack of adequate safeguards under UK law, concerning overseas data disclosure, particularly in relation to national security exemptions. It recommended that the Commission should further assess and/or closely monitor these deficiencies.[355]

Due to the criticisms regarding the Commission's draft adequacy decision, some changes were made prior to its adoption on June 28, 2021. These changes were made just two days before the TCA bridging mechanism facilitating EEA-UK personal data transfers was set to expire. Significantly, the current adequacy decision does not include transfers of personal data to the UK for immigration control purposes. This comes after a ruling by the Court of Appeal which found the immigration exemption in the UK DPA 2018 to be unlawful.[356] The Commission has, however, indicated a willingness to reassess this exclusion once it has been remedied under UK law.[357]

In a press release accompanying the adequacy decision, the Commission stated that it was satisfied with the UK system's level of protection, even concerning surveillance measures. The Commission believes that the collection of data by UK intelligence authorities is limited to what is strictly necessary to achieve the legitimate objective in question. This is subject to prior authorisation by an independent judicial body, and individuals have the ability to seek redress via

UK, (03.03.2021), [online] [cit. 2023-11-23], Available at: https://www.ianbrown.tech/2021/03/03/the-inadequacy-of-the-eu-commissions-draft-gdpr-adequacy-decision-on-the-uk/

[355] EDPB. *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, Adopted on 13 April 2021, [online] [cit. 2023-11-23], Available at https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en

[356] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 53

[357] EUROPEAN COMMISSION. *Press Statement: Data protection: Commission adopts adequacy decisions for the UK*, 28 June 2021

the UK Investigatory Powers Tribunal.[358] Nevertheless, criticism has been raised that the Commission did not adequately examine UK law to ensure it complied with EU law. This could lead to a legal challenge and the same outcome as the Safe Harbor and its successor, Privacy Shield, where adequacy decisions were revoked.[359]

The most relevant challenge for the adequacy decision is, however, the many times mentioned periodic review of adequacy decisions, as it may prove unstable in the future, when being reassessed by the Commission. For this reason, adequacy decisions are called "*living*" documents.[360] To this end, the adequacy decision will automatically expire on 27 June 2025, if the Commission has not made a renewed finding of adequacy by then.[361]

This reflects the Commission's awareness that as a third country the UK could seek to diverge from the GDPR and its other international obligations. As Vera Jourova explained, "*we have listened very carefully to the concerns expressed by the Parliament, the Member States and the European Data Protection Board, in particular on the possibility of future divergence from our standards in the UK's privacy framework*".[362]

The UK's inconsistent stance on the European Convention on Human Rights has not gone unnoticed by the Commission.,[363] in the statement attached to the draft decision the Commission stated: "*The UK is – and has committed to remain – party to the European Convention on Human Rights and to Convention 108 of the Council of Europe…Continued adherence to such international conventions is of particular importance for the stability and durability of the proposed adequacy findings*".[364] It is clear that withdrawal from the European Convention on

---

[358] EUROPEAN COMMISSION. *Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom,* (notified under document C(2021)4800), C/2021/4800, Official Journal L 360, para 275

[359]DOUWE Korff. *The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Executive Summary*, (3 March 2021), [online] [cit. 2023-11-27], Available at: https://www.ianbrown.tech/wp-content/uploads/2021/03/KORFF-The-Inadequacy-of-the-EU-Commn-Draft-GDPR-Adequacy-Decision-on-the-UK-210303final.pdf; MANANCOURT Vincent, UK data flows get Brussels' blessing, with caveats, Politico, 17 April 2021, [online] [cit. 2023-11-03], Available at: https://www.politico.eu/article/uk-privacy-data-flows-europe-blessing-caveats/

[360] EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World*, (2017) 7 Final, European Commission, 10 January 2017, p. 8–9

[361] EUROPEAN COMMISSION. *Commission Implementing Decision (EU) 2021/1772 of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom,* (notified under document C(2021)4800), C/2021/4800, Official Journal L 360, para 289.

[362] EUROPEAN COMMISSION. *Press Release: Data protection: Commission adopts adequacy decisions for the UK*, 28 June 2021, [online] [cit. 2023-11-18], Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183

[363] BOWCOTT, Owen. *UK government plans to remove key human rights protections*, The Guardian, 13 September 2020, [online] [cit. 2023-11-18], Available at: https://www.theguardian.com/law/2020/sep/13/uk-government-plans-to-remove-key-human-rights-protections

[364] EUROPEAN COMMISSION. *Press Release: Data protection: European Commission launches process on personal data flows to the UK*, 19 February 2021, [online] [cit. 2023-11-18] Available at:

Human Rights and/or the jurisdiction of the associated court, or other changes to the UK legal framework, e.g. in relation to surveillance laws, onward transfers of data to third countries, or differing judicial interpretations by UK courts of fundamental concepts such as the definition of personal data, or failure to revise the UK DPA 2018 in light of ECtHR and CJEU judgments such that the UK no longer provides an adequate level of protection, could lead to a timely review of the adequacy decision and its revocation or non-renewal.[365]

3.6.1. Longer-term: continued alignment or divergence

Evidently, Brexit has added complexity to the UK, EU, and global data protection landscape. In the TCA, both parties assert their independence several times, particularly from a regulatory standpoint. However, when it comes to data protection, the reality is quite different. The UK legal framework is put in a position of dependence on the EU framework, that cannot be avoided.[366]

Indeed, whilst the UK government's announcement that it "*intends to expand the list of adequate destinations in line with our global ambitions and commitment to high standards of data protection*",[367] will be welcomed by, Brexit supporters, seeking evidence of the UK reclaiming its sovereignty and boldly striving to forge new or stronger trade links with countries beyond the EU. However, it is important to understand that if the UK were to grant adequacy status to countries that the EU has not found adequate, and allow those adequacy regulations to be used as a "*back door*" for transferring data from EU/EEA countries that would violate GDPR requirements, it could put the UK's own adequacy status at risk. Of course, as a sovereign third country, the UK can revise the UK GDPR and UK DPA 2018, but significant divergence could jeopardise the EU-UK adequacy decision or impede its renewal. [368]

The prospect of the UK´s power diverge is hence best described as illusory. Correspondingly, as predicted, the ICO can only participate as an "observer" in EDPB meetings, Brexit has in fact reduced the UK to a "*rule taker*" instead of a rule-maker in respect of EU data protection law.[369]

---

https://ec.europa.eu/commission/presscorner/detail/en/IP_21_661

[365] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 54

[366] CELESTE, op. cit. 314, p. 12

[367] ICO and DCMS. *Joint Statement: Secretary of State for the Department for Digital, Culture Media and Sport and the Information Commissioner sign Memorandum of Understanding on data adequacy*, 19 March 202, [online] [cit. 2023-11-18], Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/

[368] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 55

[369] Ibid

Again, constraints and dependencies have led some to question whether the UK should pursue regulatory divergence in the longer term. The PM at that time, Boris Johnson, a supporter the "Leave campaign", has indicated such an intention in a written statement: "*The UK will in future develop separate and independent policies in areas such as [...] data protection.*"[370] Likewise, The UK's Secretary of State for Digital, Culture, Media, and Sport, Oliver Dowden MP, noted that: "*The EU doesn't hold the monopoly on data protection. So, having come a long way in learning how to manage data risks, the UK is going to start making more of the opportunities. Right now, too many businesses and organisations are reluctant to use data – either because they don't understand the rules or are afraid of inadvertently breaking them. That has hampered innovation and the improvement of public services and prevented scientists from making new discoveries. Clearly, not using data has real-life costs.*"[371]

Speculation that the UK will seek to create its own data protection path has been fuelled by such comments. A proposal has been put forward to replace the UK GDPR with a new "*framework for data protection*" that would inter alia reduce reliance on consent by placing greater emphasis "*on the legitimacy of data processing*", and removing Article 22 from the UK GDPR. The focus would shift to whether "*automated profiling meets a legitimate or public interest test*". This would reduce compliance burdens and foster innovation using personal data.[372]

The UK is not the only one expressing frustration with the GDPR. A review conducted two years after its implementation found that "*some stakeholders report that the application of the GDPR is challenging especially for small- and medium-sized enterprises (SMEs)*",[373] a concern that was also identified in the UK National Data Strategy.[374] Axel Voss, MEP, one of the strongest proponents of the GDPR has also asserted that "*the GDPR is not made for blockchain, facial or voice recognition, text and data mining [. . .] artificial intelligence*".[375] He argues that the GDPR,

---

[370] PM Boris Johnson. *PM Statement, UK / EU relations: Written statement – HCWS86*, 3 February 2020, [online] [cit. 2023-11-23] Available at https://questions-statements.parliament.uk/written-statements/detail/2020-02-03/HCWS86

[371] DOWDEN Oliver. *New approach to data is a great opportunity for the UK post-Brexit*, Financial Times, 27 February 2021, [online] [cit. 2023-11-23], Available at: https://www.ft.com/content/ac1cbaef-d8bf-49b4-b11d-1fcc96dde0e1

[372] The Taskforce on Innovation, Growth and Regulatory Reform (TIGRR). *Independent Report, (16 June 2021)*, [online] [cit. 2023-11-23], Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994125/FINAL_TIGRR_REPORT__1_.pdf, p. 49–53.

[373] EUROPEAN COMMISSION. *Communication from The Commission To The European Parliament And The Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation*, COM (2020) 264 final, Brussels, 24.6.2020, [online] [cit. 2023-11-23], Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264

[374] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 59

[375] ESPINOZA Javier, *EU must overhaul flagship data protection laws, says a 'father' of policy*, Financial Times, 3 March 2021, [online] [cit. 2023-11-23], Available at: https://www.ft.com/content/b0b44dbe-1e40-4624-bdb1-e87bc8016106

"*makes it impossible to properly use or even develop these technologies – AI needs access to data for training purposes, yet the vast majority of data is being stored outside the EU, which risks making it impossible for us to be competitive in any form of digital innovation, undermining our future economic prosperity*."[376]

The author disagrees, in the author's opinion, some of the criticisms are unfounded, or at least indicate a misunderstanding of how data can be processed in compliance with the GDPR. As per the Commission's suggestion, small and medium-sized enterprises (SMEs) should be provided with additional support such as templates, hotlines, and appropriate training to enable them to understand and fulfil their GDPR obligations.[377] It's important to note that while the GDPR may seem like it impedes innovation, it actually contains many "*white spaces*" and wide exemptions for research. These exemptions, if properly developed, will help support the UK's world-leading research efforts.[378]

If the issues related to supporting SMEs can be resolved, along with the development of guidance by the ICO on how data controllers and processors in the UK should interpret the exceptions and "*white spaces*" in the GDPR, then global data controllers are unlikely to demand significant deviation from the GDPR by the UK government. This will happen only if the regulation continues to meet their needs This is because significant divergence could lead to revocation or failure to renew the EU-UK adequacy decision, resulting in additional compliance burdens, which would be an unwelcome business cost. Accordingly, given that customers increasingly value high levels of data protection, it may not be appropriate for the UK to diverge significantly from the GDPR.[379] Therefore, multi-national companies operating in both the EU and UK are more likely to promote continued compliance with the GDPR than a multiplicity of different standards.[380]

If the UK decides to diverge from the GDPR in the future, there are various ways in which this could occur. One option for the UK could be to adopt a similar approach to Canada by seeking a partial adequacy decision. This would involve seeking adequacy only for the private sector, while adopting a lower standard such as Convention 108+ for other personal data processing. This option could be considered since the UK has already ratified Convention 108+. However, doing so would

---

[376] VOSS Axel. *How to bring GDPR into the digital age*, Politico, 25 March 2021, [online] [cit. 2023-11-24] Available at: https://www.politico.eu/article/gdpr-reform-digital-innovation/

[377] EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM (2020) 264 final, Brussels, 24.6.2020, p. 9

[378] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 57

[379] ICO. *Information Commissioner's Office Information Rights Strategic Plan: Trust and Confidence*, July 2020

[380] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 58

require at least two parallel standards of privacy and data protection in the UK, meaning a high-level, GDPR-compliant protection for data that is the subject of EU-UK adequacy decision transfers for the private sector, and a separate, lower (e.g., modernised-Council of Europe Convention 108) level of protection for the rest.[381]

As a possible alternative, The UK could prioritize compliance with Convention 108+ over GDPR and diverge entirely. Pursuing this course of action could lead to the GDPR losing its influence over time, not just in the UK, but other countries as well.[382]

Nonetheless, from the author's perspective, it is improbable that there will be a significant effort from the UK to deviate from the standards of the European Union, as long as the EU continues to be an essential trading partner for the UK and multinational companies worldwide continue to abide by the EU standards.

3.7. Conclusion of the Chapter

Despite lengthy and at times irreconcilable negotiations, the EU and the UK did eventually agree on the terms of a Trade and Cooperation Agreement. The UK has kept GDPR in domestic law and applied for an EU adequacy decision after acknowledging that bespoke arrangements would not be entertained. In that respect, The GDPR adequacy framework has been successful in preventing several difficult implications that would have arisen if adequacy had not been granted. The extra-territorial provisions and mutual adequacy obligations in both the UK GDPR and GDPR have established conditions for synergy and continued alignment between the two data protection frameworks.. [383]

In terms of personal data protection, Brexit was clearly a step backwards for the UK. However, it increased the level of complexity of data protection law by triggering the introduction of two parallel sets of laws potentially applying to the same subjects. By virtue of the extraterritorial application of the UK and EU GDPR, companies established in one jurisdiction but offering goods and services or monitoring the behaviour of data subjects in another jurisdiction must comply with both laws.[384] The era of unrestricted flows of personal data across the Channel is now definitely over. The TCA makes clear that the UK will have no special status as a former Member State, but will be treated in the same way as other third countries.[385]

---

[381] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 59
[382] Greenleaf has observed that CoE Convention 108 is of increasing importance in a world in which the majority of data privacy laws already come from countries outside Europe; GREENLEAF Graham. *Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives*, 2017, UNSW Law Research Paper No.17-3, p. 2
[383] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 59
[384] CELESTE, op. cit. 314, p. 12
[385] Ibid

Brexit supporters may not be happy with the outcome, as they have been calling for complete sovereignty to be restored. However, those who advocate for data protection will appreciate the fact that the UK continues to comply with GDPR. This is a positive sign of the effectiveness of GDPR in promoting high standards of data protection in third countries around the globe. Having said that, continued compliance by the UK with the GDPR should not be taken for granted. On the contrary, it must remain fit for purpose.[386]

Correspondingly, the EU should not ignore the concerns raised that it hinders innovation and competitiveness. If concerns surrounding trade and market forces are not addressed, it is possible that in the longer term, organizations may diverge from EU data protection law. If this occurs, the EU may not achieve its goal of the GDPR becoming the "global, digital gold standard of data protection".[387]

[386] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 251, p. 57
[387] Ibid, p. 60

Conclusion

Overall, this thesis dissected and established relevant legislation concerning personal data protection in the EU, focusing on the legal framework of international personal data transfers and as well as outlining relevant legislation regarding personal data protection and international personal data transfers in the UK. The thesis specifically focused on the concept of international data transfers afforded by the EU data protection law and its impact on third countries as sort of a "rule-maker"[388] with respect to the international standard of personal data protection.

The thesis focused on an overview and comparison of different methods and instruments used for transferring personal data outside the EU, afforded by the EU law, more precisely by the GDPR, and their strengths and weaknesses.

Furthermore, the thesis zeroed in on the situation of the UK, as a former EU Member State, which, by leaving the EU, had to bear the significant consequences of this decision. The consequences impacted, in the context of this thesis, the future data protection relationship between the UK and the EU, notably in the area of personal data transfers. In particular, the thesis focuses on the analysis of obtaining the UK adequacy decision, the actions of both parties involved, their outcomes, and their legal and consequential implications.

Subsequently, the thesis analysed the impact of the EU´s bargaining power in comparison to third countries, when enforcing its personal data transfer regime, the developments of the UK´s stance on its future trade agreement with the EU and its implications on data protection and personal data transfers. Afterwards, the thesis discussed the possibilities for future divergence of the UK from the EU legal framework regarding data protection and personal data transfers.

The thesis also presented relevant case law by the ECtHR and the CJEU, the European Commission and ICO Opinions, and the relevant UK legislation, as well as political statements of the UK government. Doing so it provided legal and factual context and allowed the author to isolate essential conditions that would ensure that both third countries in general, and the UK in particular, could ensure an adequate level of personal data protection by the EU so-called "golden standard"[389].

The thesis focused on the research question of whether the UK is adhering to the EU personal data protection framework post-Brexit. The author deems that if the UK maintains its legal and regulatory framework aligned with the GDPR and duly enforces compliance through the ICO as an independent regulatory authority, then the UK's adequacy shall persist. This, in the

[388] DE HERT, GONZÁLEZ-FUSTER, and VAN BRAKEL, op. cit. 230, p. 55
[389] Ibid, p. 38

author's point of view, should be among the UK´s key priorities when proceeding with its own legal framework after leaving the EU. The ICO so far has been deemed to be a strong regulator when enforcing the GDPR regime.[390] However, there still might be a possible divergence in the future, as the UK Adequacy undergoes a periodical review and there is no assurance, that it will not be revoked in the future. However, the author views the European Commission´s adequacy assessments problematic as well, as they lack transparency and may seem to be swayed by political and economic reasons, more than just simple adherence to personal data protection rules.

Some guidance is available; however issue of transparency may cause continuing uncertainty and, therefore, higher costs for companies located in third countries, resulting in an undesirable eventuality of moving their processing or even entire businesses to the EU Single Market.[391] The UK may also be struggling with political questioning of the UK Adequacy regime and its implications of obedience towards the EU framework and EU authorities.

As the UK Adequacy may not be everlasting, it is important to take into account other possibilities afforded to third countries that do not have a positive adequacy decision at all or had the positive adequacy decision revoked. Most alternative mechanisms require close cooperation with the EDPB and would entail much higher costs, especially for private organisations. Thus, EU data protection advocates have rightly framed the UK's continued compliance with the GDPR as the first evidence of the EU's potential to set standards for data protection law and promote harmonisation at a global level, but its longer-term future is less certain as the GDPR may lose influence over time if it is not fit for purpose. That is why the UK has left the EU, but not EU data protection law, at least for now. Ironically, Brexit will not achieve its long-awaited goal of freeing UK data protection law from the grip of EU law. In the Trade and Cooperation Agreement, both the UK and the EU reiterate their mutual independence multiple times, especially from a regulatory point of view, but the personal data protection reality reveals a different story.[392]

[390] RIENKE, op. cit. 6, p. 75
[391] Ibid
[392] CELESTE, op. cit. 314, p. 12

List of common abbreviations

AI – meaning the Artificial Intelligence

APPI – meaning the Act on the Protection of Personal Information (Japan)

Art. 29 WP – meaning the Article 29 Working Party

AG – meaning the Advocate General of European Court of Justice of the European Union, unless specified

BCRs – meaning the Binding Corporate Rules

Brexit – meaning the Britain´s Exit from the EU

CETA – meaning the Comprehensive Economic Trade Agreement

CETS – meaning the Council of Europe Treaty Series

CFR/Charter – meaning the Charter of Fundamental Rights of the European Union

CJEU/CJEU and Court – meaning the Court of Justice of the European Union, unless specified otherwise

CoE – meaning the Council of Europe

Convention 108 – meaning the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe)

Commission – meaning the European Commission

DCMS – meaning the Department for Digital, Culture Media and Sport (UK)

DPA - meaning the Data Protection Authority

DPPEC Regulations/DPPEC – meaning the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (UK)

DPO - meaning the Data Protection Officer

DPD – meaning the Data Protection Directive

EEA – meaning the European Economic Area

EFTA – meaning the European Free Trade Association

EC - meaning the European Community

ECHR – meaning the European Convention on Human Rights

ECtHR - meaning the European Court of Human Rights

EDPB - European Data Protection Board

EDPS – meaning the European Data Protection Supervisor

EP – meaning the European Parliament

EU – meaning the European Union

GDPR – meaning the General Data Protection Regulation

HM Government/HMG – meaning His Majesty's Government (UK)

ICC - meaning the International Chamber of Commerce

ICCPR – meaning the International Covenant on Civil and Political Rights

ICO - meaning the Information Commissioner´s Office (UK)

MEP – meaning the Member of European Parliament

NGOs – meaning Non-governmental organisations

OECD – meaning the Organisation for Economic Cooperation and Development

OCT – meaning the overseas countries and territories

OMR – meaning the outer most region

PPC – meaning the Personal Information Protection Commission (Japan)

SMEs – meaning Small and medium sized enterprises

SCCs – meaning Standard Contractual Clauses

Member State – meaning the Member state of the European Union

TCA – meaning the Trade and Cooperation Agreement (UK)

TEU – meaning the Treaty on European Union

TFEU - meaning the Treaty on the Functioning of the European Union

UDHR – meaning the Universal Declaration of Human Rights

UK DPA 2018 – meaning theData Protection Act 2018 (UK)

WP29 – meaning the Working Party on the Protection of Individuals with regard to the Processing of Personal Data

WTO - meaning the World Trade Organization

Bibliography

1. Books

BRADFORD Anu. *The Brussels Effect: How the European Union Rules the World*, (OUP, 2012), Oxford Academic, 19 Dec. 2019, ISBN 9780190088613

DE HERT, Paul; GONZÁLEZ-FUSTER, Gloria a VAN BRAKEL, Rosamunde. *Research handbook on privacy and data protection law: values, norms and global politics.* Cheltenham, England: Edward Elgar Publishing, 2022. ISBN 1-78643-851-8

Handbook on European data protection law [online]. 2018. Luxembourg: Publications Office of the European Union, 2018 ISBN 978-92-9491-901-4. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbookdata-protection_en.pdf

HARDING, Luke, *The Snowden Files: The inside story of the world's most wanted man*, Vintage Books, 2016, ISBN 100804173524

KAMARA, Irene, Eleni KOSTA a Ronald LEENES. *Research handbook on EU data protection law*. Northampton, MA: Edward Elgar Publishing, 2022, 1 online resource (664 pages). ISBN 1-80037-168-3

KRZYSZTOFEK, Marius. *Post-Reform Personal Data Protection in the European Union. General Data Protection Regulation (EU) 2016/679.* Kluwer, Alphen aan den Rijn, 2017, ISBN 9789041162427

KUNER, Christopher. (2009), *Developing an Adequate Legal Framework for International Data Transfers.* In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (eds) Reinventing Data Protection?. Springer, Dordrecht, ISBN 978-1-4020-9497-2

KUNER Christopher (2013), *Transborder data flows.* Oxford University Press, Oxford, ISBN 9780191758898

MÜLLER Patrick and FALKNER Gerda, *The EU as a policy exporter? The conceptual framework*, in Gerda Falkner and Patrick Müller (eds), EU Policies in a Global Perspective: Shaping or Taking International Regimes, London: Routledge, 2014, ISBN 9781315867410

NAEF, Tobias. *Data Protection without Data Protectionism The Right to Protection of Personal Data and Data Transfers in EU Law and International Trade Law*. Cham: Springer International Publishing, 2023. ISBN 3-031-19893-X

NOUWT S. (2009) *Towards a common European approach to data protection: a critical analysis of data protection perspectives of the Council of Europe and the European Union*. *In: Gutwirth S, Poullet Y, de Hert P et al (eds) Reinventing data protection?* Springer, Heidelberg, ISBN 978-1-4020-9498-9

REINKE, Guido. *Blue Paper on Data Protection: Data Transfer between the European Union and third countries: Legal options for data controllers and data processors in a post-Brexit Britain*. London: GOLD RUSH Publishing, 2019. ISBN 1908585102

SUDA, Yuko. *The Politics of Data Transfer: Transatlantic Conflict and Cooperation over Data Privacy (Routledge Studies in Global Information, Politics and Society)*. New York: Routledge, 2017. ISBN 1138696285

WEBER, Rolf H. and Dominic STAIGER. *Transatlantic Data Protection in Practice*. Zurich, Switzerland: Springer, 2017. ISBN 3662572338

2. Articles

BENDIEK A. and RÖMER M. *Externalizing Europe: the global effects of European data protection,* 2019, Digital Policy, Regulation and Governance, ISSN 2398-5046, Emerald, Bingley, Vol. 21

CELESTE Edoardo, *Cross-border data protection after Brexit*, DCU Brexit Institute Working Paper Series, No 4/2021

EDMUNDSON A, ENSAFI R, FEAMSTER N, REXFORD J *Characterizing and avoiding routing detours through surveillance states*, 2016, Princeton University

GREENLEAF, Graham. *International Data Protection Agreements after the GDPR and Schrems, (2016) 139 Privacy Laws & Business International Report 12-15*. 1. Australia: UNS Law Research Paper No. 2016-29, 2016

GREENLEAF Graham. *Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives*, 2017, UNSW Law Research Paper No.17-3

GREENLEAF, Graham. *Questioning 'Adequacy'*. UNSW Law Research Paper No. 18-1. 2018

HUSTINX Peter. *EU Data Protection Law: The Review of Directive 95/46/EC and the General Data Protection Regulation.* New Technologies and EU Law. Oxford University Press, 2017

HON, W. Kuan. *Data localization laws and policy. The EU data protection international transfers restriction through a cloud computing lens.* Edward Elgar, Cheltenham, 2017

KIRBY, Michael. (2011) *The history, achievement and future of the 1980 OECD guidelines on privacy*, International Data Privacy Law, Volume 1, Issue 1, February 2011, Pages 6–14

KUNER Christopher*, A Court of Justice International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15*, EU-Canada PNR, (2018) CML Rev, 55(3)

KUNER Christopher*, A Court of Justice International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15*, EU-Canada PNR, (2018) CML Rev, 55(3)

LYNSKEY Orla, *Extraterritorial Impact in Data Protection Law through an EU Law Lens*, DCU Brexit Institute Working Paper Series – No 8/2020

MEUNIER, Sophie and NICOLAIDIS, Kalypso. *The European Union as a conflicted trade power*. Routledge, Taylor&Francis Group. 2006

MURRAY, Andrew, *Data transfers between the EU and UK post Brexit?*, (2017) International Data Privacy Law, Volume 7, Issue 3

PAPAKONSTANTINOU, Vagelis and DE HERT, Paul. *The PNR Agreement And Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework On Either Side Of The Atlantic*, 2009, CML Rev, 46(3)

PHILLIPS, Mark. *International data-sharing norms: from the OECD to the general data protection regulation(GDPR)*, Hum Genet 137(8), 2018

PLOMAN, Edward W. *International law governing communications And information*, Greenwood Press, Westport, 1982

SIMITIS S, DAMMANN U. *EU-Datenschutzrichtlinie Nomos*, Baden-Baden, 1997

TAMBOU Olivia*, Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights,* European Foreign Affairs Review, 2018

TAMBOU, Olivia. *The French adaptation of the GDPR*. In: McCullagh K, Tambou O, Bourton S (eds) National adaptations of the GDPR. Blogdroiteuropéen, Luxembourg, 2019

TZANOU, Maria. *The fundamental right to data protection. Normative value in the context of counter-terrorism surveillance*. Hart, Oxford, 2017

3. Electronic sources

BAINES Jon, DE REYA Mischon, quoted in Sam Clark. *No SCCs needed for data controllers governed by GDPR*, ICO lawyer suggests, Global Data Review Blog 12 October 2018, [online] [cit. 2023-11-03], Available at: https://globaldatareview.com/article/no-sccs-needed-data-controllers-governed-gdpr-ico-lawyer-suggests

BAKER, Jennifer. *What does the newly signed 'Convention 108+' mean for UK adequacy?* IAPP (International Association of Privacy Professionals), IAPP (International Association of Privacy Professionals), 2018, 30. October 2018, [online] [cit. 2023-10-19], Available at: https://iapp.org/news/a/what-does-the-newly-signed-convention-108-mean-for-u-k-adequacy/

BOFFEY Daniel, Brussel seeks to tie UK to European human rights court after Brexit, The Guardian, 18 June 2018, [online] [cit. 2023-11-03 Available at: https://www.theguardian.com/law/2018/jun/18/brussels-seeks-to-tie-uk-to-european-human-rights-court-after-brexit

BOWCOTT, Owen. *UK government plans to remove key human rights protections*, The Guardian, 13 September 2020, [online] [cit. 2023-11-23], Available at: https://www.theguardian.com/law/2020/sep/13/uk-government-plans-to-remove-key-human-rights-protections

BROWN, Ian and KORFF, Douwe. *The inadequacy of UK data protection law Part One: General inadequacy*, [online] [cit. 2023-11-23], Available at: https://www.ianbrown.tech/wp-content/uploads/2020/10/Korff-and-Brown-UK-adequacy.pdf,

BUGHIN, Jacques a Susan LUND. The ascendancy of international data flows. Vox EU, McKinsey Global Institute [online]. 2017, 2017 [cit. 2023-08-03]. Available at: https://www.mckinsey.com/mgi/overview/in-the-news/the-ascendancy-of-international-data-flows

CASTRO Daniel, *Brexit Allows UK to Unshackle Itself from EU's Cumbersome Data Protection Rules*, Centre for Data Innovation, 20 July 2016, [online] [cit. 2023-11-18] Available at: https://datainnovation.org/2016/07/brexit-allows-uk-to-unshackle-itself-from-eus-cumbersome-data-protection-rules/

CYBERMATRON. *Data protection in the EU-UK Withdrawal Agreement - Are we being framed?*, Cybermatron Blog, 15 November 2018, [online] [cit. 2023-11-18], Available at https://cybermatron.blogspot.com/2018/11/data-protection-in-eu-uk-withdrawal.html

DOWDEN Oliver, *New approach to data is a great opportunity for the UK post-Brexit*, Financial Times, 27 February 2021, Available at: https://www.ft.com/content/ac1cbaef-d8bf-49b4-b11d-1fcc96dde0e1, Accessed 27 November 2023

EARDLEY, Nick. *Tories could campaign to leave European human rights treaty if Rwanda flights blocked*, BBC News, 9 August 2023, [online] [cit. 2023-12-03], Available at: https://www.bbc.com/news/uk-politics-66438422

ESPINOZA, Javier. *EU must overhaul flagship data protection laws, says a 'father' of policy*, Financial Times, 3 March 2021, [online] [cit. 2023-11-23], Available at: https://www.ft.com/content/b0b44dbe-1e40-4624-bdb1-e87bc8016106

GOVE, Michael, *Why I'm backing Brexit*, The Spectator, 20 February 2016, [online], [cit. 2023-11-18], Available at: https://www.spectator.co.uk/article/michael-gove-why-i-m-backing-brexit/

GREAVES, Paul a Wim NAUWELAERTS. Privacy, Cyber & Data Strategy Advisory: EU-U.S. Data Privacy Framework vs. EU Standard Contractual Clauses for Transatlantic Transfers of Personal Data. *ALSTON&BIRD* [online]. USA: ALSTON&BIRD LLP., 2023, 5 [cit. 2023-10-20], Available at :https://www.alston.com/en/insights/publications/2023/09/eu-us-data-privacy-framework

JONES, Joe. Infographic: *Global data transfer contracts*. Iapp [online]. 2023, 2023 [cit. 2023-08-03]. Available at: https://iapp.org/resources/article/infographic-global-data-transfer-contracts/

MANANCOURT Vincent, *UK data flows get Brussels' blessing, with caveats*, Politico, 17 April 2021, [online] [cit. 2023-11-03], Available at: https://www.politico.eu/article/uk-privacy-data-flows-europe-blessing-caveats/

OECD Privacy. OECD.org [online]. [cit. 2023-11-14]. Available at: https://www.oecd.org/digital/privacy/

SEONG, Jeongmin, WHITE, Olivia, WOETZEL Jonathan, SMIT Sven, DEVESA, Tiago BIRSHAN, Michael and SAMANDARI, Hamid. *Global flows: The ties that bind in an interconnected world: Discussion paper. McKinsey Global Institute* [online]. 2022, 2022 [cit.

2023-08-03]. Available at: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/global-flows-the-ties-that-bind-in-an-interconnected-world#/

TRENTMANN, Nina. Companies Weigh Data-Privacy Risks Ahead of Brexit. *Wall Street Journal* [online]. Wall Street Journal, 2019, **1**(1), 1 [cit. 2023-10-20]. Available at: https://www.wsj.com/articles/companies-weigh-data-privacy-risks-ahead-of-brexit-11552363260

VOSS, Axel, *How to bring GDPR into the digital age*, Politico, 25 March 2021, [online] [cit. 2023-11-24] Available at: https://www.politico.eu/article/gdpr-reform-digital-innovation/

WHITE Michael, *Why John Whittingdale is politically tone deaf and 30 years out of date*, The Guardian Blog, 9 March 2016, [online] [cit. 2023-11-18], Available at: https://www.theguardian.com/politics/blog/2016/mar/09/why-john-whittingdale-is-politically-tone-deaf-and-30-years-out-of-date

4. EU Treaties and legislative material

Agreement on the European Economic Area of 2 May 1992 [1994] Official Journal L 1/3

Charter of Fundamental Rights of the European Union. OJ C 326, 26.10.2012, p. 391–407. Cited as "Charter" or "CFR"

Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012, p. 47–390. Cited as "TFEU"

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50. Cited as "DPD"

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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), OJ L 119, 4.5.2016, p. 1–88. Cited as "GDPR"

EEA Joint Committee (1999) Decision No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement, [2000] OJ L 296/41, EEA Joint Committee (2018) Decision No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement, [2018] OJ L 183/23

4.1. Commission Decisions

2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441), Official Journal L 215, 25.8.2000

2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, Official Journal L 215, 25.8.2000

2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, Official Journal L 2, 4.1.2002

2003/490/EC: Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, Official Journal L 168 , 5.7.2003

2003/821/EC: Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey, Official Journal L 308, 25.11.2003

2004/411/EC: Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man, Official Journal L 151, 30.4.2004

2008/393/EC: Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey, Official Journal L 138, 28.5.2008

2010/625/EC: Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra, Official Journal L 277, 21.10.2010

2011/61/EU: Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, Official Journal L 27, 1.2.2011

2013/65/EU: Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, Official Journal L 28, 30.1.2013

2016/1250/EC: Commission Implementing Decision (EU) of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176). OJ L 207, 1.8.2016

2018/1907/EC: Decision (EU) 2018/1907 — conclusion of the Agreement between the EU and Japan for an Economic Partnership, Official Journal L 330, 27.12.2018

2019/419/EU: Commission Implementing Decision (EU) of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, Official Journal L 76/1

2021/1773/EC: Commission Implementing Decision (EU) of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom, notified under document C(2021) 4801, Official Journal of the European Union L 360/69

023/1795/EC: Commission Implementing Decision of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework notified under document C(2023) 4745, Official Journal of the European Union OJ L 231

5. UK Treaties and legislative material

The Data Protection Act 2018, 23 May 2018, Cited as “UK DPA 2018”

Statutory Instruments 2019 No. 419. Exiting the European Union Data Protection Electronic Communications, The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, 28th February 2019

European Union (Future Relationship) Act 2020, Cited as “Trade and Cooperation Agreement” or the “TCA”

6. Other treaties and national legislation

COUNCIL OF EUROPE, European Convention on Human Rights, CETS No. 005, 1950

COUNCIL OF EUROPE. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), entry in force 1 October 1985. Cited as “Convention 108”

COUNCIL OF EUROPE. Protocol Amending the Protection of Individuals with regard to Automatic Processing of Personal Data of 10 October 2018 (CETS No. 223)

COUNCIL OF EUROPE. Chart of signatures and ratifications of Treaty 223. In: Council of Europe. Coe.int [online]. 2023, 2023-10-19 [cit. 2023-10-19]. Available at: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223

Titre V Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés; CNIL (2019) Available at : https://www.legifrance.gouv.fr/loda/id/LEGISCTA000037817604

UNITED NATIONS GENERAL ASSEMBLY. *The Universal Declaration of Human Rights*, Paris, 10 December 1948, General Assembly resolution 217 A

7. Case-law

7.1. EU

7.1.1. Judgements

Case C-465/00, C-138/01 and C-139/01, Österreichischer Rundfunk and others, ECR 2003 p. I-4989, ECLI:EU:C:2003:294, [2003], [CJEU]

Case C-101/01, Lindqvist, ECR 2003 p. I-12971 ECLI:EU:C:2003: 596, [2003] [CJEU]

Case C-400/10 PPU J. McB v L.E, ECLI:EU: C:2010:582, [2010], [CJEU]

Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC], ECLI:EU:C:2014:317, [2014], [CJEU]

Case C-362/14 Maximillian Schrems v Data Protection Commissioner ECLI:EU:C:2015:650 [2015], [CJEU]

Case C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce, ECLI:EU:C:2017:197, [2017], [CJEU]

Opinion 1/15, ECLI:EU:C:2017:592 [2017], [CJEU]

Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems ECLI:EU:C:2020:559 [2020], [CJEU]

Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, ECLI:EU:C:2020:790, [2020], [CJEU]

7.1.2. Opinions of Advocate General

Joined Cases C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010

Case C-311/18, Opinion of Advocate General Saugmandsgaard, Schrems II: CJEU, 19 December 2019, Schrems II, EU:C:2019:1145

7.2. ECtHR Judgements

Case of Klass and others v Federal Republic of Germany, Judgment, Merits, App no 5029/71 (A/28), (1979-80) 2 EHRR, 214, IHRL 19 (ECHR 1978), 6th September 1978, European Court of Human Rights [ECHR]

Case of Malone v. The United Kingdom (Application no. 8691/79), Judgment Strasbourg, 2 August 1984, European Court of Human Rights [ECHR]

CASE OF L.H. v. LATVIA (Application no. 52019/07) JUDGMENT STRASBOURG 29 April 2014 FINAL 29/07/2014, European Court of Human Rights [ECHR]

Case of ROMAN ZAKHAROV v. RUSSIA, App no 47143/06, JUDGMENT STRASBOURG 4 December 2015, European Court of Human Rights [ECHR]

Case of Big Brother Watch and Others v. the United Kingdom, App no 58170/13, 62322/14 and 24960/15, ECHR 2018, GRAND CHAMBER 2021, 25th May 2021, European Court of Human Rights [ECHR]

8. Non-legislative material from EU bodies

ARTICLE 29 WORKING PARTY, *Adequacy Referential (2018), wp254rev.01*, Available at: https://ec.europa.eu/newsroom/article29/items/614108

EUROPEAN COMMISSION. *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield* [online]. IP/16/216. Strasbourg. 2016. [cit. 2023-10-20]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216

EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World*, (2017) 7 Final, European Commission, 10 January 2017

EUROPEAN COMMISSION. *Framework for the future relationship: Police and judicial cooperation in criminal matters, Task force for the Preparation and Conduct of the Negotiations with the United Kingdom under Article 50 (TEUTF 50),* 12 July 2017 TF50 (2017) 8/2 – Commission to UK

EUROPEAN COMMISSION. *Letter on cross-border data flows and EU trade agreements*, 1 Mar. 2018, [online], [cit. 2023-10-23], Available at: http://data.consilium.europa.eu/doc/document/ST-6687-2018-INIT/en/pdf

EUROPEAN COMMISSION. *Speech by Michel Barnier at Business Europe Day 2018, Brussels*, 1 March 2018, [online], [cit. 2023-10-23], Available at: http://europa.eu/rapid/press-release_SPEECH-18-1462_en.html

EUROPEAN COMMISSION. *The European Union and Japan decide to create the world´s largest area of safe data flows*, press release, IP/18/4501 (Tokyo), 17 July 2018

EUROPEAN COMMISSION. *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation - version adopted after public consultation,* 2016/679

EUROPEAN COMMISSION. *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation*, 2016/679

EUROPEAN COMMISSION. *Horizontal Provisions on Cross-border Data Flows and Personal Data Protection*, news release of 18 May 2018, [online], [cit. 2023-10-23], Available at: https://ec.europa.eu/newsroom/just/items/627665

EUROPEAN COMMISSION. *Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom*, 2019/C 384 I/02, Official Journal 2019 C 384 I/02

EUROPEAN COMMISSION. *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation,* 2016/679

EUROPEAN COMMISSION. *Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM (2020) 264 final, Brussels, 24.6.202

EUROPEAN COMMISSION. *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S.*

Secretary of Commerce Gina Raimondo, [online]. STATEMENT/21/1443. Brussels. 2021. [cit. 2023-10-20]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/statement_21_1443

EUROPEAN COMMISSION. *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, 13 April 2021

EUROPEAN COMMISSION. *Factsheet: Trans-Atlantic Data Privacy Framework [online]. Brussels*. 2022. [cit. 2023-10-20]. Available at: https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/TransAtlantic%20Data%20Privacy%20Framework.pdf.pdf

EUROPEAN COMMISSION. *Press Release: Data protection: Commission adopts adequacy decisions for the UK*, 28 June 2021, [online], [cit. 2023-10-20], Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183

EUROPEAN COMMISSION. *Data Protection -Standard Contractual Clauses for Transferring Personal Data to Non-EU Countries (Implementing Act), (Have your say)*, [online], [cit. 2023-10-20], Available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

EUROPEAN COMMISSION. *EU horizontal provisions on Cross-border data flows and protection of personal data and privacy in the Digital Trade Title of EU trade agreements*, [online], [cit. 2023-10-23] Available at: https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_1462

EUROPEAN COMMISSION. *How the EU determines if a non-EU country has an adequate level of data protection*, [online], [cit. 2023-10-23], Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

EUROPEAN COMMISSION. *Standard Contractual Clauses (SCC) - Standard contractual clauses for data transfers between EU and non-EU countries. European Commission,* [online]. 2023, 1 [cit. 2023-10-20]. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

EUROPEAN COMMISSION. *New Standard Contractual Clauses - Questions and Answers overview - Frequently asked questions on the new SCCs. European Commission*, 2023

EUROPEAN COMMISSION. *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection*. In: EUROPEAN COMMISSION. Commission.europa.eu [online]. 2023, 2023 [cit. 2023-10-19]. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

EUROPEAN COMMISSION. *New Standard Contractual Clauses - Questions and Answers overview - Frequently asked questions on the new SCCs. European Commission* [online]. European Commission, 2023, 1 [cit. 2023-10-20]. Available at: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en#:~:text=Standard%20contractual%20clauses%20%28SCCs%29%20are%C2%A0standardised%C2%A0and%C2%A0pre-approved%20model%20data%20protection,arrangements%20with%20other%20parties%2C%20for%20instance%20commercial%20partners

EUROPEAN CONVENTION. *Explanations relating to the Charter of Fundamental Rights*, Official Journal C 303, 14.12.2007

EUROPEAN PARLIAMENT. *LIBE Committee Briefing: Personal data protection achievements during the legislative term 2014–2019: the role of the European Parliament*, April 2019, [online], [cit. 2023-10-23], Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/608870/IPOL_BRI(2019)608870_EN.pdf

9. Non-legislative material from UK bodies

DCMS. *Explanatory Framework for Adequacy Discussions, Section A: Cover Note*, 13 March 2020

DCMS. *Memorandum of Understanding on the role of The ICO in relation to New UK Adequacy Assessments*, 19 March 2021, [online], [cit. 2023-10-23], Available at: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments

DExEU. *The exchange and protection of personal data - a future partnership paper*, 24 August 2017, [online], [cit. 2023-11-18], Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

HM GOVERNMENT. *Framework for the UK-EU partnership – Data Protection, presentation prepared by the UK negotiating team*, May 2018

HM GOVERNMENT. *Technical Note: Benefits Of A New Data Protection Agreement*, 7 June 2018, [online], [cit. 2023-11-18], Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714677/Data_Protection_Technical_Note.pdf

HM GOVERNMENT. *Department for Exiting the European Union, The Exchange and protection of personal data: A future partnership paper*, 24 August 2018

HM GOVERNMENT. *Response to the Committee on Exiting the European Union Seventh Report of Session 2017–18, The Progress of the UK's negotiations on EU withdrawal: Data* (HC 1317, 6 Sept. 2018), [online], [cit. 2023-11-18], Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmexeu/1564/156402.htm

HM GOVERNMENT, DEXEU. *Department for Exiting the European Union, EU Withdrawal Bill, Withdrawal Agreement*, 21 November 2018

HM GOVERNMENT. *Explanatory framework for adequacy discussions*, 13 March 2020, [online], [cit. 2023-11-18], Available at: https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions

HOUSE OF COMMONS LIBRARY. *Brexit: red lines and principles", Briefing paper by Vaughne Miller*, number 7938, 21 June 2017

HOUSE OF COMMONS. *Exiting the European Union Select Committee, The progress of the UK´s negotiations on EU withdrawal: Data*, Seventh Report of the Session 2017-19, report together with formal minutes relating to the report, HC 1317, 3 July 2019

HOUSE OF COMMONS LIBRARY. *Research Briefing: Statistics on UK-EU trade* 10 November 2020, [online], [cit. 2023-11-18]Available at: https://commonslibrary.parliament.uk/research-briefings/cbp-7851/

HOUSE OF LORDS, *European Union Committee, Brexit: the EU data protection package*, 3rd Report of Session 2017–19 – published 18 July 2017 – HL Paper 7

ICO. *The eighth data protection principle and international data transfers*. Version 4.1., 30 June 2017

ICO. *Information Commissioner's Office Information Rights Strategic Plan: Trust and Confidence*, July 2020

ICO and DCMS. *Joint Statement: Secretary of State for the Department for Digital, Culture Media and Sport and the Information Commissioner sign Memorandum of Understanding on data adequacy*, 19 March 2021 [online], [cit. 2023-11-27], Available at: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/

ICO. *Overview – Data Protection and the EU: What if we lose adequacy?* In: Information Commissioner´S Office - ICO. Ico.org.uk [online]. 2023, 2023-10-19 [cit. 2023-10-19]. Available at: https://ico.org.uk/for-organisations/data-protection-and-the-eu/overview-data-protection-and-the-eu/#lose-adequacy

THE TASKFORCE ON INNOVATION, GROWTH AND REGULATORY REFORM (TIGRR). *Independent Report, 16 June 2021),* [online], [cit. 2023-11-27], Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994125/FINAL_TIGRR_REPORT__1_.pdf

10. Other non-legislative materials

EDPS. *EDPS Opinion on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement*, Opinion 3/2021, 22 February 2021, [online], [cit. 2023-11-27], Available at: https://edps.europa.eu/system/files/2021-02/2021_02_22_opinion_eu_uk_tca_en.pdf

EDPB. *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, Adopted on 13 April 2021, [online], [cit. 2023-11-27], Available at https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en

FEDERATION OF SMALL BUSINESSES, 'Manifesto European Elections 2014, February 2014

GOVERNMENT OF CANADA.*The European Union's General Data Protection Regulation*. Tradecommissioner.gc.ca [online]. 2023, [cit. 2023-11-27]Available at: https://www.tradecommissioner.gc.ca/guides/gdpr-eu-rgpd.aspx?lang=eng

OECD. *Explanatory Memorandum. Guidelines governing the protection of privacy and transborder flows of personal data*. Annex to the recommendation of the Council of 23 September 1980

OECD. *The OECD Privacy Framework: Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ("Privacy Guidelines"), revised recommendations*, OECD Working Party on Information Security and Privacy, 2013

OECD, Declaration on Government Access to Personal Data Held by Private Sector Entities, OECD/LEGAL/0487, [online]. [cit. 2023-11-14], Available at: , https://legalinstruments.oecd.org/en/instruments/OECDLEGAL-0487

OLIVER PATEL. *Statement made by Oliver Patel, Head of Inbound Data Flows, Department for Digital, Culture, Media and Sport (DCMS) at Commercial data transfers between the UK and EU and the adequacy decision, Cross DPN Online Workshop*, 22 April 2021

PM BORIS JOHNSON. *PM Statement, UK / EU relations: Written statement – HCWS86*, 3 February 2020, [online], [cit. 2023-11-27], Available at: https://questions-statements.parliament.uk/written-statements/detail/2020-02-03/HCWS86

PM THERESA MAY. *PM´s Florence Speech: a new era of cooperation and partnership between the UK and the EU, speech transcript*, (PM Theresa May, 22 September 2017)

PM THERESA MAY. *PM´s speech at Munich Security Conference, speech transcript* (PM Theresa May, 17 February 2018)

Mezinárodní předávání osobních údajů mimo Evropskou unii

Abstrakt

Tato práce rozebírá právní koncepty ochrany soukromí a osobních údajů, právní rámec EU, konkrétně relevantní primární právo a sekundární právo EU, jako jsou směrnice o ochraně údajů a obecné nařízení o ochraně údajů. Práce se dále zabývá konceptem mezinárodního předávání osobních údajů mimo Evropskou Unii a právním základem tohoto předávání, upraveným v obecném nařízení o ochraně údajů, jeho jednotlivými metodami a jejich srovnáním ve vztahu k jejich oblasti působnosti a konkrétnímu využívání. Za zásadní považovala autorka vymezení rozhodnutí o odpovídající ochraně, proces udělení takového rozhodnutí a jeho kritéria. Následně se práce zabývala představením vhodných záruk, jako alternativních metod mezinárodního předávání osobních údajů dle práva EU.

Těžištěm práce je představit režim třetí země na příkladu Spojené království Velké Británie a Severního Irska, jakožto bývalého členského státu EU. Práce se v tomto směru zabývá vývojem britského práva na ochranu osobních údajů z hlediska mezinárodního předávání údajů po brexitu. Práce se věnovala jednáním mezi Spojeným královstvím a EU na téma jejich dohody o obchodu a spolupráci. Zvláštní pozornost byla věnována vymezení podmínek zachování adekvátní ochrany osobních údajů, poté co se Spojené království odchýlilo od unijního právního rámce pro ochranu osobních údajů.

V závěru práce se autorka zabývá konkrétním rozhodnutím o odpovídající ochraně, uděleným Spojenému království Evropskou komisí a jeho pravděpodobnou budoucí stabilitou. Autorka se zaměřuje na otázku budoucích možných přístupů k otázce zajištění přiměřené úrovně ochrany osobních údajů, které by mohly mít v budoucnu zásadní vliv na režim obchodu a spolupráce mezi Evropskou Unií a Spojeným královstvím.

Autorka věří, že provedení takovéto analýzy a syntézy a následného zhodnocení umožnilo do hloubky rozebrat a objasnit podmínky a nezbytná opatření pro mezinárodní předávání osobních údajů mimo Evropskou Unii, zejména do Spojeného království. Autorka se dále domnívá, že proces vyjednávání režimu budoucího obchodu a spolupráce, popsaný na případu Spojeného království, může sloužit jako referenční příklad do budoucna, pokud by se taková situace v EU opakovala.

Klíčová slova: Ochrana údajů, právo EU, mezinárodní předávání údajů, ochrana osobních údajů ve Spojeném království, Brexit, odpovídající úroveň ochrany údajů, rozhodnutí o odpovídající ochraně

Cross-border data flows from the EU: Data protection and the right to privacy

Abstract

This thesis discusses the legal concepts of privacy and personal data protection, the EU legal framework, specifically the relevant primary law and secondary EU law such as the Data Protection Directive and the General Data Protection Regulation. The thesis further examines the concept of international transfers of personal data outside the European Union and the legal basis for such transfers, as regulated by the GDPR, its different methods and their comparison in relation to their scope and specific use. The author considered the definition of the adequacy decision, the process of granting such a decision and its criteria to be essential. Subsequently, the thesis dealt with the presentation of appropriate safeguards as alternative methods of international transfers of personal data under EU law.

The focus of the thesis is to introduce the third country regime using the example of the United Kingdom of Great Britain and Northern Ireland as a former EU Member State. In this respect, the thesis examines the development of UK data protection law in terms of international data transfers after Brexit. The thesis has looked into the negotiations between the UK and the EU on their trade and cooperation agreement. Particular attention has been paid to defining the conditions for maintaining adequate data protection after the UK has departed from the EU legal framework for data protection.

Finally, the author concludes the thesis by examining the specific adequacy decision granted to the UK by the European Commission and its likely future stability. The author focuses on the question of possible future approaches to ensuring an adequate level of protection for personal data, which could have a major impact on the trade and cooperation regime between the European Union and the United Kingdom in the future.

The author believes that conducting such an analysis and synthesis and subsequent evaluation has enabled the conditions and necessary arrangements for international transfers of personal data outside the European Union, in particular to the United Kingdom, to be analysed and clarified in depth. Furthermore, the author believes that the process of negotiating a future trade and cooperation regime, as described in the case of the United Kingdom, can serve as a reference example for the future, should such a situation be repeated in the EU.

Keywords: Data protection, EU law, international data transfers, Brexit, personal data protection in the UK, Brexit, data protection adequacy, adequacy decision