10
Data Protection

Edoardo Celeste

1. Introduction

With Brexit, the United Kingdom (UK) is leaving a space where personal data has freely circulated since 1995, where companies are subject to uniform rules, and where national data protection authorities cooperate in a coordinated manner. As stated by Fabbrini, with Brexit, 'for the first time a Member State has decided of its own accord to exit what is admittedly the most successful project of regional and economic integration'.[1] This is particularly visible in the field of data protection. It was never necessary to build a tunnel physically under the English Channel to allow for the free flow of personal data between the UK and other European Union (EU) Member States. Yet, the complexity of the legal engineering governing what was until 31 December 2020 a seamless exchange of data across the English Channel is not to be underestimated. The 1995 Data Protection Directive affirmed the principle of free flow of personal data among EU Member States, prohibiting all sorts of restrictions. Indeed, all of the pre-existing pan-European instruments, namely the non-legally binding 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data and the 1981 Council of Europe Convention No 108 for the protection of individuals with regard to the processing of personal data, still foresaw, in their original version, a number of exceptions that Member States could adopt to restrict the free flow of data, even among states party to the OECD or which have ratified the Convention No 108.[2] Conversely, the Data Protection Directive, in line with the then European Community's objective of establishing a single market, for the first time created a multinational space of free movement of personal data that could sustain the needs of the European

[1] Federico Fabbrini, 'Introduction' in Federico Fabbrini (ed), ***The Law & Politics of Brexit. Volume II: The Withdrawal Agreement*** (Oxford University Press 2020) 1.

[2] See art 17 of the OECD Guidelines and art 12 of the Council of Europe Convention No 108/1981.

Edoardo Celeste, *Data Protection* In: *The Law & Politics of Brexit*. Edited by: Federico Fabbrini, Oxford University Press.
 DOI: 10.1093/oso/9780192848468.003.0010

internal trade while, at the same time, ensuring a high level of protection of fundamental rights.[3]

The UK, by leaving the EU, has now regressed to the status of a third country which does not automatically benefit from a *de jure* recognition of the legal standards afforded to the protection of personal data, and consequently precludes the unhindered flow of information from other EU Member States. EU personal data cannot be freely transferred to the UK unless through the use of specific legal mechanisms.[4] However, the EU-UK Trade and Cooperation Agreement (TCA) signed on 24 December 2020 soothed this harsh transition through the introduction of a six-month interim period, during which the UK was not considered to be a third country and data could continue to be freely transferred across the English Channel.[5] Within this timeframe, the European Commission worked hard to adopt, in a record time and despite mounting criticism, a decision recognizing the adequacy of UK data protection law and allowing for a free transfer of data between the EU and the UK under the GDPR.[6] However, this adequacy decision, adopted only two days before the end of the interim period on 28 June 2021, is still subject to periodic reviews and exposed to potential legal challenges that can undermine the stability of cross-border data flows between the EU and the UK.

This chapter aims to reconstruct how the UK data protection framework has evolved in the last four years, from the time of the Brexit referendum to the conclusion of the TCA. It will assess to what extent the new UK data protection regime reflects the Brexit desiderata, and analyses the challenges of the future relationship between the UK and the EU in light of the solutions envisioned by the TCA.

The chapter will be divided into three parts, corresponding to the three main phases of the Brexit process from a data protection perspective. Section 2 will analyse the Brexit negotiations before the adoption of the TCA. It will explain the importance of the data protection question during the Brexit negotiations, and reconstruct the development of UK data protection law from 2016 to 2021. Section 3 will focus on the TCA and the six-month transitional period this established, during which the Commission worked to adopt an adequacy

[3] See Rolf H Weber, 'Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives' (2013) **3** ***International Data Privacy Law*** 117.

[4] GDPR, arts 45 ff.

[5] See art 782, text available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:22021A0430(01)&from=EN.

[6] EU Commission, *Commission implementing decision of 28.6.2021 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* https://ec.europa.eu/info/sites/default/files/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

decision. It will examine the terms of the TCA related to the digital field and, in particular, the TCA's final provisions specifically regulating the transition of the UK to the status of a third country with regard to data transfers. Finally, section 4 will consider Brexit's consequences from a data protection standpoint, with particular focus on data transfers across the English Channel and the recent EU Commission's adequacy decision. It will be argued that the adequacy decision will not provide the UK with the desired level of regulatory emancipation advocated by Brexit supporters nor will it offer a stable and reliable mechanism for data transfers. Indeed, the adequacy mechanism will subject the UK legal system to regular monitoring by the EU that will restrict the UK's ability to develop freely its own data protection framework for fear of losing the EU adequacy status. Moreover, in light of the recent Court of Justice of the EU (CJEU) case law on data transfers and data retention, a UK adequacy decision will naturally be exposed to the risk of being invalidated owing to the non-conformity of the UK national security regime with EU law. The chapter will conclude with an explanation of why Brexit manifestly represents a step backwards from a data protection perspective.

2. Data Protection in the Brexit Negotiations

This section will reconstruct the legal framework on the free flow and protection of personal data during the Brexit negotiations until the adoption of the TCA. It aims to offer a comprehensive view of the status quo related to the EU-UK data protection relations at the end of the transition period on 31 December 2020. The section will be divided into two parts: first, it will outline the importance of the free flow of data and data transfers in the Brexit negotiations and, secondly, it will analyse how UK data protection legislation has evolved over the last five years.

2.1 Relevance of the Data Protection Question

What can be referred to as the 'data protection question' was central to the Brexit negotiations. EU data protection law provides for the unhindered flow of personal data within the European Economic Area (EEA), comprising the EU Member States, Norway, Iceland, and Liechtenstein.[7] Personal data transfers

[7] GDPR, art 1(3).

to third countries are conversely allowed only in limited circumstances. More specifically, a general green light for data exchanges with third countries may be given by the EU Commission through the adoption of a decision declaring, in light of a general assessment of the legal system, the adequacy of the data protection framework of the receiving country.[8] The UK, by leaving the EU, obtains the status of a mere third country and is subject to such rules. As a consequence, the free flow of personal data between the UK and the EU is not automatically guaranteed, and can only occur if the EU Commission adopts an adequacy decision. Otherwise, personal data can be exchanged on a case by case basis under one of the specific exceptions established by EU data protection law in relation to cross-border data transfers.[9]

With regard to the free flow of personal data, the UK's status after Brexit is certainly more precarious. Cross-border data transfers are no longer free, but must be supported by a specific legal instrument or provision. Moreover, even if backed by the adoption of an adequacy decision by the EU Commission allowing for a general transfer of data from the EU to the UK, such exchange is subject to the mutable nature of adequacy decisions, which are, by rule, subject to periodical updates and, occasionally, exposed to potential legal challenges and to the stricter examination of the CJEU. However, the dramatic nature of the new data protection scenario created by Brexit cannot truly be appreciated if one does not highlight the crucial role played by the exchange of personal data from the point of view of commercial relations and other forms of non-commercial cooperation between the UK and the EU. Only in this way can one fully understand why, as de Hert and Papakonstantinou wrote in the aftermath of the Brexit referendum, 'data protection has the potential to be among the issues that "make" or "break" a possibly successful Brexit'.[10]

The months preceding the Brexit referendum in 2016 and the first phase of Brexit were characterized by animated discussions on the advantages and disadvantages of the UK's exit from the EU.[11] A plurality of figures and percentages describing the current trade relations with the EU and non-EU countries, as well as speculation on the potential future trade flows of the UK were used to support opposite theories. As regards the relevance of the flow of personal data across the English Channel, however, reports and figures conveyed a univocal

[8] ibid art 45.

[9] ibid arts 46 ff.

[10] Paul de Hert and Vagelis Papakonstantinou, 'The rich UK contribution to the field of EU data protection: Let's not go for "third country" status after Brexit' (2017) **33** ***Computer Law & Security Review*** 354.

[11] See Kalypso Nicolaïdis, 'The Political Mantra: Brexit, Control and the Transformation of the European Order' in Federico Fabbrini (ed), ***The Law & Politics of Brexit*** (Oxford University Press 2017).

message: the profoundly intertwined architecture of the EU-UK trade relations as well as other forms of cooperation in a plurality of fields, such as law enforcement and intelligence sharing, rely heavily on the exchange of personal data and would significantly suffer in case of a sudden hindrance to that flow.[12]

First, from a general commercial perspective, the 27 EU Member States together represent the UK's top trading partner, involving more than half of the UK's trade in goods, including both imports and exports.[13] Trade relations represent the basis, if not the essence, of personal data transfers, especially in the contemporary context of a data-driven economy.[14] It is therefore not surprising that the overwhelming majority of the personal data exchanged by the UK with foreign countries, including both movements from and to the UK, is with the 27 remaining EU Member States.[15] Secondly, if one analyses the nature of the UK's top businesses, the crucial role played by the exchange of personal data is apparent.[16] The service industry is dominant, with a significant role played by financial services firms, which rely heavily on data exchange.[17] The UK has until now acted as the European hub for banks, payment service providers, and, more recently, fintech companies, many of which are incorporated outside of the EU but have their European headquarters in London.[18] Moreover, according to 2017 data, over the past few years the UK has given birth to almost half of European large digital companies.[19]

At the same time, besides the commercial elements of data exchange between the EU and the UK, it is important to underline the crucial role that cross-border data transfer plays from a law enforcement and intelligence perspective.[20] Historically, both the EU and the UK have been equally committed

[12] UK Department for Digital, Culture, Media and Sport, 'Explanatory framework for adequacy discussions: Section A: covering note' (13 March 2020) https://www.gov.uk/government/publications/explanatory-framework-for-adequacy-discussions.

[13] Issam Hallak, 'Future EU-UK Trade Relationship' **European Parliament** (2020) Briefing PE 646.185 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/646185/EPRS_BRI(2020)646185_EN.pdf; UK Department for Exiting the European Union, 'The exchange and protection of personal data: a future partnership P paper' (2017) https://www.gov.uk/government/publications/the-exchange-and-protection-of-personal-data-a-future-partnership-paper.

[14] Vincenzo Zeno-Zencovich, 'Free-Flow of Data: Is International Trade Law the Appropriate Answer?' in Federico Fabbrini, Edoardo Celeste, and John Quinn (eds), ***Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*** (Hart Publishing 2021); Paul Hofheinz and David Osimo, 'Making Europe a Data Economy: A New Framework for Free Movement of Data in the Digital Age' **The Lisbon Council** (2017) Policy Brief 11(1) https://lisboncouncil.net/wp-content/uploads/2020/08/LISBON-COUNCIL-Making-Europe-A-Data-Economy.pdf.

[15] Kathryn Wynn, 'Brexit: if it ain't broke, why break it?' (2019) **20** ***Privacy and Data Protection*** 11.

[16] See further the chapter by Niamh Moloney in this volume.

[17] Karen McCullagh, 'Brexit: potential trade and data implications for digital and "fintech" industries' (2017) 7 ***International Data Privacy Law*** 3.

[18] ibid.

[19] UK Department for Exiting the European Union (n 13).

[20] See further the chapter by Oliver Garner in this volume. See also Deirdre Curtin, 'Brexit and the EU Area of Freedom, Security and Justice: Bespoke Bits and Pieces' in Federico Fabbrini (ed), ***The Law***

to the fight against terrorism and serious crime. The presence of a great number of financial companies on British soil makes the UK an invaluable mine of sensitive information for carrying out investigations related to financial crimes and terrorism in other EU Member States.[21]

For all of these reasons, laying the foundations for a solid and stable partnership with the EU on the protection and exchange of personal data has been a priority for the UK since the beginning of the Brexit process.[22] Moreover, following the same rationale, after the end of the transition period, the UK promptly authorized data transfers to the EEA, while the EU Commission worked hard to adopt in a record time an adequacy decision under the GDPR allowing for the free movement of data from the EEA to the UK, as we will examine in more detail in the next sections.[23]

2.2 UK Legislation after Brexit

To complete the overview of the status quo of the Brexit data protection question, it is useful to analyse the evolution of UK data protection law from the Brexit referendum to the end of the transition period.

In 2016, the same year as the Brexit referendum, EU data protection law made the most significant change since the time of the introduction of the Data Protection Directive in 1995 by adopting the General Data Protection Regulation (GDPR), the first EU legal instrument regulating the protection and free flow of personal data that is directly applicable in all EU Member States.[24] The GDPR entered into force on 23 May 2018, and, on the same date, the UK introduced the Data Protection Act 2018. This statute aimed to provide a single source for codified data protection law in the UK. First, it supplemented the GDPR in areas where the EU regulation allowed Member States to legislate further, such as on processing conditions for special categories of data (Article 9 GDPR) or on derogations to data subject rights (Article 23 GDPR).[25]

& Politics of Brexit (Oxford University Press 2017); Anne Weyembergh, 'Consequences of Brexit for European Union criminal law' (2017) **8** ***New Journal of European Criminal Law*** 284; Stefania Paladini and Ignazio Castellucci, ***European Security in a Post-Brexit World*** (Emerald 2019).

[21] UK Department for Exiting the European Union (n 13).

[22] ibid.

[23] ICO, 'International Transfers after the UK Exit from the EU Implementation Period' (4 March 2021) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/ accessed 12 March 2021.

[24] Regulation (EU) 2016/679 (General Data Protection Regulation).

[25] Data Protection Act 2018, pt 2, ch 2.

Secondly, it applied a limited set of GDPR norms to rare cases of processing falling outside the scope of the GDPR, such as to public authorities processing personal data in unfiled papers or to bodies other than law enforcement or intelligence authorities processing data for national security or defence purposes.[26] Thirdly, it implemented the Law Enforcement Directive into UK law,[27] regulating data processing of law enforcement authorities.[28] Fourthly, it established a legal framework for personal data processed by intelligence agencies.[29]

Looking more broadly at the evolution of UK law after Brexit, from a data protection perspective it is also important to mention significant changes in the legislation on access and retention of personal data by national security authorities. In the aftermath of the CJEU decision in *Digital Rights Ireland*, which led to the invalidation of the Data Retention Directive, the UK adopted the Data Retention and Investigatory Powers Act (DRIPA) 2014 to continue the effects of the Data Retention Regulations 2009 which implemented the defunct EU directive.[30] The DRIPA 2014, originally adopted in the form of emergency legislation, expired at the end of 2016 and was replaced by the Investigatory Powers Act (IPA) 2016. Almost simultaneously, however, as we will examine in more detail in section 4.2, in the *Tele2 Sverige and Watson* case the CJEU found that the UK general and indiscriminate data retention and access regime established by the DRIPA 2014 was not in line with EU fundamental rights, thus de facto making the provisions of the newly enacted IPA 2016 void.[31]

This legal regime was in force until Exit Day. The European Union (Withdrawal) Act 2018, provides that at the end of the transition period, direct EU legislation in force on Exit Day, including regulations such as the GDPR and EU Commission adequacy decisions, is incorporated into UK law as 'retained EU law'.[32] The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, however, effectual from Exit Day, modify the version of the GDPR introduced into UK law, the so-called

[26] ibid pt 2, ch 3. This is the so-called 'applied GDPR'.
[27] Directive (EU) 2016/680 (Law Enforcement Directive).
[28] Data Protection Act 2018, pt 3.
[29] ibid pt 4.
[30] Eleni Kosta, 'The Retention of Communications Data in Europe and the UK' in Lilian Edwards (ed), ***Law, Policy, and the Internet*** (Hart Publishing 2018).
[31] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige* ECLI:EU:C:2016:970; Xavier Tracol, 'The judgment of the Grand Chamber dated 21 December 2016 in the two joint *Tele2 Sverige* and *Watson* cases: The need for a harmonised legal framework on the retention of data at EU level' (2017) **33** ***Computer Law & Security Review*** 541.
[32] European Union (Withdrawal) Act 2018, s 3.

UK GDPR, and amends the Data Protection Act 2018 in order to provide a more coherent legal framework.[33]

The UK GDPR no longer includes references to the EU, EU bodies, and Member States, only alluding to the UK and its institutions. It applies only to the UK, but maintains the provisions allowing for extraterritorial application that are present in the EU GDPR and, consequently, is applicable to data controllers and processors established in the EEA that process data of UK residents while offering them goods or services or while monitoring their behaviour.[34] Moreover, it transfers powers previously entrusted to the EU Commission to the relevant UK Secretary of State.[35]

The Data Protection Act 2018, as amended by the 2019 Regulations, no longer presents two separate sections respectively complementing the GDPR and 'applying' it beyond its original scope of application. Its parts implementing the Law Enforcement Directive and regulating data processing by intelligence agencies are maintained, while a single regime (UK GDPR) is established for all remaining kinds of data processing.[36] The 2019 Regulations also revoke all of the EU Commission's adequacy decisions, which were incorporated into UK law as 'direct EU legislation'. The Data Protection Act 2018 now temporarily authorizes data transfers to countries deemed adequate by the EU Commission prior to Exit Day, together with the EU Member States and states comprising the EEA, until the norm will be repealed by the applicable minister.[37]

If, on the one hand, the 2019 Regulations make the UK internal data protection framework more coherent, on the other hand, UK and EU companies will potentially have to comply with two different legal systems after Exit Day. The extraterritorial scope of application of both the EU and the UK GDPR compel companies addressing data subjects residing in the other jurisdiction to apply both regimes and, potentially, to be subject to the enforcement of two different, but no longer coordinated, data protection authorities.[38]

[33] See the Keeling Schedules of the UK GDPR and the Data Protection Act 2018 at https://www.gov.uk/government/publications/data-protection-law-eu-exit.

[34] UK GDPR, art 3. Cf on the topic Fabbrini, Celeste, and Quinn (n 14).

[35] For example, the power of adopting adequacy decisions for cross-border data transfers according to art 45 UK GDPR.

[36] See the Keeling Schedule of the Data Protection Act 2018 at https://www.gov.uk/government/publications/data-protection-law-eu-exit.

[37] Data Protection Act 2018, s 213.

[38] See Vincent Manancourt, 'What the interim Brexit data flows deal means for Britain' ***POLITICO*** (28 December 2020) https://www.politico.eu/article/what-the-interim-brexit-data-flows-deal-means-for-britain/ accessed 20 January 2021.

3. The TCA and the New Transitional Period

On 24th December 2020, only seven days before the end of the transition period established by the Withdrawal Agreement, the EU and the UK concluded a Trade and Cooperation Agreement (TCA) to avoid a no deal Brexit.[39] The TCA defined mutual commitments in the digital field, and opened a new transitional period to address the question of personal data transfers from the EU to the UK. The following sections will analyse the terms of the TCA and its final provisions on data transfers.

3.1 Terms of the TCA

The TCA avoided a 'no-deal Brexit'. In the field of data protection, a no-deal Brexit would have impacted thousands of businesses through a sudden stop of free cross-border data flows from the EU to the UK unless specific legal mechanisms supporting the transfer were in place, such as binding corporate rules or standard contractual clauses. Not to mention other sectors where the exchange of data across the English Channel is of vital importance, including the law enforcement and judicial cooperation field.

The TCA, introduced a series of trade barriers (Part Two) when compared with the status enjoyed by the UK as an EU Member State.[40] Part Two, Title III regulates digital trade, i.e. trade carried out by 'electronic means'.[41] In this section, Chapter 2 focuses on cross-border data flows and data protection. The EU and the UK made a formal commitment to ensure data flows, avoiding the imposition of localization requirements for data, equipment, and networks.[42] Both parties shall recognize and protect the right to data protection and privacy in order to enhance the level of trust among market actors.[43] The EU and the UK are free to design their legal frameworks regulating data protection and flows independently, but are compelled to guarantee a regime of data transfer of general application within the digital market.[44]

[39] See further the Introduction by Federico Fabbrini in this volume.
[40] See further the chapter by Paola Mariani and Giorgio Sacerdoti in this volume.
[41] TCA, art 197.
[42] ibid art 201. Cf Edoardo Celeste and Federico Fabbrini, 'Competing Jurisdictions: Data Privacy Across the Borders' in Grace Fox, Theo Lynn, and Lisa van der Werff (eds), ***Data Privacy and Trust in Cloud Computing*** (Palgrave 2020).
[43] TCA, art 202(1).
[44] ibid art 202(2).

Part Three of the TCA focuses on law enforcement and judicial cooperation.[45] Both parties commit to protecting personal data along with other fundamental rights.[46] Swift—but no longer direct or real-time—mechanisms to allow the exchange of DNA profiles, fingerprints, and vehicle registration numbers (so-called Prüm data), passenger name records (PNR) data, and criminal records will be put in place.[47] In particular, the TCA reiterates the need to ensure respect for data protection principles, such as security and retention limitation, with regard to these data. After Exit Day, the UK no longer participates in the working of Europol and Eurojust nor does it have direct access to the Schengen Information System (SIS), but cooperation frameworks have been established to fill this gap.[48]

3.2 The TCA's Final Provisions on Data Protection

The core parts of the TCA did not deal with the main conundrum of the data protection question, i.e. the mechanism for supporting data transfers between the EU and the UK. To address this issue, the negotiators instead included a transitional agreement in the TCA's final provisions. This agreement was valid only in relation to data transfers and did not postpone the entry into force of the UK GDPR, as provided by the 2019 Regulations. As a consequence, all obligations linked to the emergence of this new, independent law apparatus, such as for instance the need to adopt a UK representative for non-EU companies trading in the EU and UK, became effective on 1 January 2021.

Article 782 provided that transfers of data between the EU and the UK could continue for up to six months as if the UK were not a third country.[49] This clause opened a new transitional phase in relation to data protection whose aim was twofold: on the one hand, it prevented a sudden halt of data flows between the EU and the UK; on the other hand, it provided the EU Commission with sufficient time to adopt an adequacy decision. Indeed, the TCA explicitly provided that this transitional period would have ended as soon as an adequacy decision is adopted, or, failing that, after six months, whichever occurs earlier.[50] In this way, by referring to its intention to adopt an adequacy decision,

[45] See further the chapter by Oliver Garner in this volume.
[46] TCA, arts 524 and 525.
[47] TCA, pt III, Titles II, II.I and IV.
[48] ibid pt III, Titles V and VI. See further the chapter by Oliver Garner in this volume.
[49] Technically, four months subject to a two-month tacit extension (ibid art 782(4)(b)).
[50] ibid art 782(4).

the EU Commission also clarified the potential future relationship between the EU and the UK from a data protection perspective. The former EU Member State will not enjoy any special status, such as a binding bilateral recognition of adequacy, as originally proposed by the UK during the negotiations.[51] The European Data Protection Supervisor affirmed that this transitional status should not constitute precedent for future trade agreements.[52]

From a data protection perspective, this solution determines a break between EU and UK legal systems, which, at least in theory, are free to develop independently without being bound by the specific architecture of a chosen trade model. This divorce remains, however, only on paper. The trade relationships between EU and UK compel their respective data protection systems to cohabit, if not to act in a synchronized manner. Definitively not a decisive emancipation for the suffering spouse, at least from a data protection perspective. Indeed, the new transition period during which the UK was not considered as a third country for data transfer purposes was subject to the condition that UK data protection law be frozen as of December 2020.[53] The purpose of this clause was apparent: avoiding a UK recently freed from the EU marital control revolutionizing its data protection regime, and thus frustrating the work of the EU Commission in issuing an adequacy decision. More specifically, until June 2021, the UK was required to limit itself to keeping its data protection regime in line with the EU regime, for example recognizing the new Standard Contractual Clauses (SCC) that the EU Commission has published in draft in November 2020,[54] and to abstain from exercising 'designated powers', such as recognizing other third countries as adequate for data transfer purposes, or approving new codes of conducts, certification mechanisms, binding corporate rules, standard contractual clauses or administrative arrangements.[55] According to the final provisions of the TCA, an exercise of these powers was theoretically permitted without triggering the end of the transitional period subject to notification to the EU, and, in case of request, prior approval of the

[51] Daniel Boffey, 'UK calls for special EU deal on data-sharing laws after Brexit' ***The Guardian*** (23 May 2018) https://www.theguardian.com/technology/2018/may/23/uk-calls-for-eu-deal-data-sharing-laws-brexit accessed 9 February 2021.

[52] European Data Protection Supervisor, Opinion 3/2021 on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement, https://edps.europa.eu/system/files/2021-02/2021_02_22_opinion_eu_uk_tca_en.pdf.

[53] TCA, art 782(1).

[54] EU Commission, 'Data protection: standard contractual clauses for transferring personal data to non-EU countries (Implementing Act)' ***Have your say*** (12 November 2020) 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 accessed 20 January 2021.

[55] TCA, art 782(3).

EU-UK Partnership Council, the governance organ created by the TCA to oversee the implementation of the agreement.[56]

However, one can observe that, even now that this 'learner's permit' phase has ended and the UK has acquired its 'full licence' to develop its data protection legal system autonomously, this will hardly grant total freedom and independence.[57] Indeed, data transfers between the EU and the UK are set to be generally permitted on the basis of an EU adequacy decision. Such an instrument is adopted unilaterally by the EU Commission subject to an assessment of the adequacy of the third country's legal system and should be regularly updated. As the next section will explore in more detail, this condition will not only prevent the UK from independently developing its data protection framework for fear of losing its status of adequacy, but will also subject areas of law that originally fell outside the scope of EU law when the UK was a Member State, such as the national security field, to EU scrutiny.

4. The New Adequacy Decision

On 28 June 2021, just two day before the end of the six months accorded by the TCA to define the question of cross-border data transfers, the EU Commission adopted two adequacy decisions in relation to the UK, respectively covering data transfers under the GDPR and the Law Enforcement Directive.[58] The EU Commission originally published the two draft adequacy decisions on 19 February 2021. After a non-binding assessment by the European Data Protection Board, the draft adequacy decisions went through the comitology procedure requiring the majority of the representatives of EU Member States to vote in favour of their adoption, a herculean process to complete before June 2021 considering that the quickest adequacy decision, which concerned Argentina, was adopted in 18 months.[59]

Certainly, the UK's nature as a former Member State of the EU, which shared the same regulatory framework until 31 December 2020 and whose data protection regime remained substantially frozen until June 2021, helped speed up

[56] ibid art 782(1), (9)–(11).

[57] See further the chapter by Brigid Laffan in this volume.

[58] See EU Commission, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, accessed 30 June 2021.

[59] 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. See Toby Helm and others, 'The Brexit deal is done: but many crucial issues are unresolved' ***The Guardian*** (27 December 2020) http://www.theguardian.com/politics/2020/dec/27/the-brexit-deal-is-done-but-many-crucial-issues-are-unresolved accessed 1 February 2021.

the procedure. On the one hand, one may think that it would be paradoxical, not to say unreasonable, to deny a green light to data transfers to a country with which personal data was freely transferred until some months ago. On the other hand, however, the UK, by leaving the EU, does not enjoy any special treatment as a former Member State. It became a third country and is subject to standard rules related to international data transfer set by Chapter 5 of the GDPR. The new status acquired by the UK makes the uncomfortable exercise of looking into the bag of the EU's formerly unsuspicious travel mate necessary, even requiring the opening of some pockets that the EU would not have had the right to access during the UK's EU membership.

This section will analyse the adequacy decision related to commercial data transfers in the broader context of the Brexit process. First, it will be argued that, from a data protection perspective, the UK will not achieve a full emancipation from the EU, being subject to broad and continued adequacy control. Secondly, it will argue that this legal solution does not lay solid foundations for a stable data transfer building, by potentially being subject to legal claims in light of the contentious nature of some areas of the UK's legal system, notably in the field of national security.

4.1 An Incomplete Emancipation: Adequacy as a Bridle

Until the first CJEU decision in *Schrems*, there was widespread belief that adequacy decisions represented definitive assessments operated by the EU Commission, following an *una tantum* analysis of the foreign legal system, which was not subject to potential contestation or disapplication from national data protection authorities.[60] In the *Schrems I* case, the CJEU debunked these assumptions.

First, adequacy decisions do not represent documents set in stone. They are supposed to be evolving instruments that reflect the current state of the foreign legal system in question. Through these mechanisms, the EU Commission certifies that a third country currently offers adequate safeguards justifying a green light to personal data transfers from the EU. This therefore implies that

[60] Case C-362/14 *Schrems* ECLI:EU:C:2015:650; Tuomas Ojanen, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter: ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner' (2016) 12 *European Constitutional Law Review* 318; Tuomas Ojanen, 'Rights-Based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union' in David Cole, Federico Fabbrini, and Stephen Schulhofer (eds), ***Surveillance, Privacy and Transatlantic Relations*** (Hart Publishing 2017).

a positive assessment of the adequacy of a foreign country could suddenly change in the event of a reform or advent of a new practice affecting the foreign data protection framework. The EU Commission explicitly acknowledged this possibility in the UK adequacy decision, providing for the possibility to suspend the decision, and inserting for the first time a sunset clause which limits the validity of the decision for a period of four years.[61] Therefore, the adoption of an EU adequacy decision in relation to the UK should not sound like an unconditional green light for Westminster. The UK, in deciding how further to develop its legal framework, will have to take into account potential effects for data protection, and appraise whether this might have an impact on the positive assessment underlying its adequacy decision. For example, the idea of negotiating a data transfer agreement between the UK and the US that would go beyond the remit of the corresponding EU instruments currently in place could per se represent the *actus reus* that, in light of the often-recognized inadequacy of the US data protection system, would be susceptible to jeopardizing the validity of an adequacy decision.[62] This possibility clearly shows the extent to which, although formally emancipated, the development of the UK data protection framework will still be de facto subject to a series of limitations indirectly deriving from the EU legal system.

Brexit is not leading to an increased level of regulatory emancipation for the UK, at least from a data protection perspective. The British desire to determine its destiny independently from the EU, which was one of the leading arguments used by Brexiteers ahead of the 2016 referendum, was explicitly frustrated by the TCA clauses requiring the UK not substantially to amend its data protection framework until an adequacy decision is issued by the EU Commission. Moreover, now that an adequacy decision has been adopted by the EU, the UK will still be de facto subject to a form of monitoring aimed at assessing the continued adequacy of its data protection system.

Secondly, adequacy decisions can be challenged in court—as Mr Schrems successfully did twice for the adequacy decision related first to the US Safe Harbour regime and then to the EU-US Privacy Shield. And their operation can be de facto suspended if national data protection authorities have doubts in relation to the adequacy of the data protection regime of the third country in question—indeed, while national data protection authorities do not have a say on the validity of the adequacy decision itself, they can suspend cross-border

[61] EU Commission (n 58) paras 285 and 289.
[62] See Manancourt (n 38).

data transfers to the interested country.[63] As the next section will explain, this is a possibility that is more than purely academic for the UK.

4.2 A Precarious Solution: The National Security Issue

After Brexit, the normative architecture supporting data transfers between the EU and the UK has not only become more complex, but also more unstable. The UK adequacy decision is exposed to a series of vulnerabilities which are rooted in the very bowels of the British legal system and emerged well before Brexit.[64] The issue lies in the powers of the UK national security agencies, which were first criticized and accused, and more recently, explicitly condemned by various supranational courts for infringing the right to privacy and data protection.[65] Paradoxically, as this section will explain, when the UK was an EU Member State, it could exploit the blurred boundaries of EU law to escape from external scrutiny, while now the mechanisms underlining adequacy decisions bring them into the spotlight.

Indeed, in *Schrems I* the CJEU affirmed that the EU Commission, when assessing the level of protection offered by a third country, shall have regard not only to the data protection framework *stricto sensu*, but also to the broader set of provisions affecting EU personal data transferred. Although the EU Commission in the UK adequacy decision underlines as a sort of pre-emptive justification that many of the most contentious aspects of the UK data protection framework will not apply to EU data transferred across the English Channel, Article 45 GDPR refers generally to a control of 'domestic law and international commitments' of the third country in question.[66] The EU Commission can issue and maintain an adequacy decision only if it is satisfied that the legal regime applicable to EU data in a third country, as a whole, offers a level of protection which is substantially equivalent to that afforded by EU law read in conjunction with the Charter of Fundamental Rights of the EU. This implies a holistic assessment of the foreign legal system focusing in

[63] *Schrems* (n 60) paras 38 ff.

[64] Andrew D Murray, 'Data Transfers between the EU and UK Post Brexit?' (2017) 7 ***International Data Privacy Law*** 149; Orla Lynskey, 'The Extraterritorial Impact of Data Protection Law through an EU Law Lens' in Federico Fabbrini, Edoardo Celeste, and John Quinn (eds), ***Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*** (Hart Publishing 2021).

[65] See also Murray (n 64), who highlights the consequences of the absence of an explicitly recognized right to data protection in UK law, equivalent to art 8 of the Charter of Fudamental Rights of the EU.

[66] EU Commission (n 58), eg recital 199.

particular on the presence of appropriate safeguards, the enforceability of data protection rights, and the effectiveness of legal remedies.[67]

The European Parliament, in a resolution adopted on 12 February 2020, had already clearly flagged the three main issues of a potential adequacy decision to the EU Commission.[68] First, the existence of a broad immigration exemption in UK data protection law. The UK Data Protection Act provides that the data subject's rights to information, access, erasure, to restrict processing, and to object may be limited where they would be likely to affect 'the maintenance of effective immigration control' and related investigations,[69] two wide categories which can be interpreted broadly and thus lead to the disapplication of a significant portion of the UK GDPR in relation to non-UK citizens. On 26 May 2021, the Court of Appeals of England and Wales held that the immigration exemption is incompatible with the UK GDPR.[70] This led the EU Commission to backtrack and exclude personal data to which the immigration exemption can apply from the scope of the adequacy decision.[71]

Secondly, the EU Parliament cast doubt on the compatibility of the UK data retention regime with the EU *acquis*. In 2016, the CJEU decided the joined cases *Tele2 Sverige and Watson*, on a reference also from the Court of Appeal of England and Wales.[72] The CJEU, echoing its previous decision in *Digital Rights Ireland*,[73] which had led to the invalidation of the Data Retention Directive, affirmed that the general and indiscriminate retention of telecommunications metadata is not permitted under EU law, and this principle applies also to national legislation implementing a no longer existing directive.[74] Indeed, *Tele2 Sverige and Watson* were related to, respectively, the Swedish and UK statutes transposing, or—more correctly in the case of the UK—continuing the effects, of the defunct Data Retention Directive, which regulated the retention of

[67] See *Schrems* (n 60) paras 75 ff.

[68] European Parliament resolution of 12 February 2020 on the proposed mandate for negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland (2020/2557(RSP). https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang = en&reference = 2020/2557. Concerns reiterated more recently in the resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (**2021/2594(RSP)** https://www.europarl.europa.eu/doceo/document/TA-9-2021-0262_EN.html.

[69] UK Data Protection Act 2018, sch 2, pt 1, para 4.

[70] Court of Appeal (Civil Division), Open Rights Group v Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport, [2021] EWCA Civ 800, para 53 ff.

[71] EU Commission (n 58), recital 6.

[72] *Tele2 Sverige* (n 31); see also Tracol (n 31).

[73] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland* ECLI:EU:C:2014:238; see also Mark D Cole and Annelies Vandendriessche, 'From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg' (2016) 2 *European Data Protection Law Review* 121.

[74] See Edoardo Celeste, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) **15** ***European Constitutional Law Review*** 134.

metadata for public security reasons, such as the fight against serious crime.[75] More recently, in October 2020, the CJEU, in the *Privacy International* case referred by the UK Investigatory Power Tribunal, the British authority examining disputes involving intelligence agencies, analysed the case of the bulk data retention system imposed by UK national security legislation.[76] Although national security is a field falling outside the scope of EU law, the CJEU ruled that a national statute, in so far as it derogates from the principle of confidentiality of electronic communications established by the e-Privacy Directive, cannot impose a regime of general and indiscriminate retention, transfer, and access to metadata for national security purposes. Once again, the CJEU reaffirmed that only a system of targeted data retention may be a justifiable compression of EU fundamental rights.[77] Lastly, on 25 May 2021, in *Big Brother Watch v UK* the Grand Chamber of the European Court of Human Rights confirmed the 2018 chamber decision affirming that the lack of legal oversight and the disproportionate breadth characterizing the British data retention regime constituted a violation of Article 8 of the ECHR enshrining the right to protection of personal and family life.[78] Despite the different approaches adopted by the CJEU and the European Court of Human Rights on the admissibility of bulk data retention in general,[79] both courts set clear limits to the powers of national security agencies, and the UK will now need to implement these judgments to have its legal system regarded as compatible with EU law, and therefore adequate.

Thirdly, the EU Parliament highlighted the related issue of mass surveillance, explicitly inviting the Commission to take into account the recent CJEU case law concerning US adequacy decisions. Indeed, in the *Schrems I* and *Schrems II* cases, respectively decided in 2015 and 2020, the CJEU invalidated the Commission's decisions declaring the adequacy of the Safe Harbour and Privacy Shield regimes, which allowed for the transfer of personal data from the EU to the US.[80] The reason that prompted these cases, and was decisive of their outcome, was the extent of power vested in US national intelligence authorities and their potential misuse of EU personal data. A consideration

[75] For a comprehensive analysis of UK data retention law see Kosta (n 30).

[76] Case C-623/17 *Privacy International* ECLI:EU:C:2020:790; see also Joined Cases C-511/18, C-512/18, and C-520/18 *La Quadrature du Net and Others* ECLI:EU:C:2020:791.

[77] See Celeste (n 74).

[78] *Big Brother Watch and Others v United Kingdom* App nos 58170/13, 62322/14, and 24960/15 (ECtHR. 25 May 2021); see Celeste (n 74).

[79] See Celeste (n 74).

[80] *Schrems* (n 60); Case C-311/18 *Facebook Ireland and Schrems* ECLI:EU:C:2020:559; see also Maria Tzanou, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' in Federico Fabbrini, Edoardo Celeste, and John Quinn (eds), ***Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*** (Hart Publishing 2021).

that might easily be called into question in relation to the UK, in light of its participation in the Five Eyes, the intelligence sharing partnership which also includes the US, Canada, Australia, and New Zealand.[81]

In conclusion, the UK adequacy decision is subject to a time bomb. Over the past few years, the case law of the CJEU has become more solid and clear in relation to the incompatibility of various practices adopted by national security authorities involving personal data. This makes the general EU-UK data transfer mechanism based on the adequacy decision unstable and unreliable. If, once again, the EU Commission has found a way to reach a compromise between commercial interests and fundamental rights, it is only a question of time before the CJEU will intervene. And in this way, paradoxically, Brexit will enhance the level of external pressure on UK national security law, a sector that, when the UK was an EU Member State, was considered as falling outside the scope of EU law and within the sovereign competences of the UK.[82]

5. Conclusion

From a data protection perspective, Brexit manifestly represents a step backwards for the UK. Brexit has increased the level of complexity of data protection law by inducing the introduction of two parallel sets of legislation potentially applying to the same actors. 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 the other, are required to comply with both laws. The era of unhindered personal data flows across the English Channel has definitively ended. The TCA clarified that the UK will not enjoy any special status as a former Member State, but will conversely be considered as other third countries are. The UK has lost direct and real time access to important databanks fed by European law enforcement agencies, and will have to rely on the standard mechanisms of transfers provided by the GDPR for the exchange of data in the commercial sector.

[81] See David Lyon, ***Surveillance after Snowden*** (Polity Press 2015); Ioanna Tourkochoriti, 'The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-E.U. in Data Privacy Protection' (2014) **36** ***University of Arkansas at Little Rock Law Review*** 161.

[82] Even the House of Lords EU Committee in its report 'Beyond Brexit: policing, law enforcement and security' (17 March 2021) https://publications.parliament.uk/pa/ld5801/ldselect/ldeucom/250/250.pdf, recognized that the UK now, as a third country, will paradoxically be subject to 'higher standards' in the field of national security, and that there is 'abundant scope for legal challenges on data protection grounds' in this area.

However, paradoxically, Brexit does not achieve any sovereigntist objective of freeing UK data protection law from the bridle of EU law. In the TCA, the parties reiterate multiple times their independence, especially from a regulatory point of view, but the data protection reality tells us a different story. The UK legal framework is inexorably put in a position of dependence. During the extra six-month transitional period lasting until June 2021 in which the EU Commission worked to adopt an adequacy decision, the UK could not significantly amend its legal regime. Even now that an adequacy decision has been adopted, UK data protection law will be subject to regular monitoring in order to assess the persistence of safeguards offering an adequate level of protection for EU personal data. In light of the recent case law of the CJEU, such continued supervision will not spare UK national security law, once solidly considered a stronghold of sovereign competence and now destined to be sifted through in order to check its compliance with the EU *acquis*.

The general EU-UK data transfer regime relying on the adequacy decision is anticipated to be precarious and unstable. Companies are advised to put in place alternative transfer mechanisms. The UK immigration exemption, the data retention regime, and the national surveillance mechanisms have already been predicted to be the Achilles' heel of the UK adequacy decision. The likelihood is high that the CJEU will soon once more 'put asunder' what the EU Commission has 'joined together' in the name of EU trade.