# INTERNATIONAL DATA TRANSFERS: THE IMPACT OF BREXIT ON THE EU-UK DATA TRANSFERS

Tereza Pechová*

***Abstract:*** *This paper examines the development of UK data protection law in terms of international data transfers after Brexit. It looks into the negotiations between the UK and the EU on their trade and cooperation agreement. Particular attention is paid to defining the conditions for maintaining adequate data protection after the UK has departed from the EU legal framework for data protection. This paper examines the specific adequacy decision granted to the UK by the European Commission and its likely future stability. Finally, the paper focuses on the question of possible future approaches to ensuring an adequate level of protection for personal data, which could have a significant impact on the trade and cooperation regime between the European Union and the United Kingdom in the future.*

***Key words:*** *Data protection, EU law, international data transfers, Brexit, personal data protection in the UK, Brexit, data protection adequacy, adequacy decision, GDPR*

## INTRODUCTION

The massive growth of international data flows leads to a 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. 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, creating a requirement for international coordination to ensure an adequate level of personal data protection. In the context of the United Kingdom (the UK), now a third country, the approach to data protection is very similar, coming from the same origin. However, with Brexit occurring and a possible divergence of the data protection legislation, a clear set of rules for such transfer must be in place to maintain the level of data protection afforded to EU citizens.

This paper focuses on whether the UK, a former Member State with nationally implemented General Data Protection Regulation (the GDPR) regime, has maintained the level of data protection regarding personal data transfers after Brexit. Furthermore, it provides an overview of the negotiations following the decision to leave the EU, measures currently in place and the discussions between the relevant data protection authorities regarding the future establishment of measures for personal data transfers.

## I. 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

* Mgr. Tereza Pechová, Graduate of Faculty of Law, Charles University in Prague, Prague, Czech Republic. ORCID: 0009-0002-5113-0676.

chose to vote for *"Leaving"* the EU.[1] The decision to leave the EU, at the time the UK's largest trading partner and one of the world's largest trading blocks,[2] was a significant historic 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.

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 entirely expected that the winning vote would be to *"leave"*.[3]

Consequently, what ensued after the referendumęs 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 UKęs 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 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 whether 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 European Economic Area (the EEA) and the UK, as well as internationally. A significant question emerged: whether to diverge, either immediately or in the longer term, from the EU data protection law.

## II. THE NEGOTIATION PERIOD

During Brexit negotiations, Prime Minister May aimed for the UK's Information Commissioner's Office, the UKęs data protection authority, (the ICO) to maintain its membership in the European Data Protection Board (the EDPB) and participate in the EU's "one-stop-shop" supervisory mechanism. PM May understood that the Court of Justice of the European Union (the CJEU) must continue to have jurisdiction over certain aspects of data protection after Brexit.[4] 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.[5]

---

[1] Brexit is a neologism of British and Exit coined in 2012 by Peter Wilding which expresses the UK's withdrawal from the EU. In: *bbc.com* [online]. 14. 3. 2019 [2024-09-17]. Available at: <https://www.bbc.com/culture/article/20190314-how-brexit-changed-the-english-language>.

[2] House of Commons Library, Research Briefing: Statistics on UK-EU trade. In: *House of Commons Library* [online]. 10. 11. 2020 [2024-09-17]. Available at: <https://commonslibrary.parliament.uk/research-briefings/cbp-7851/>.

[3] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. Research handbook on privacy and data protection law: values, norms and global politics. Cheltenham: Edward Elgar Publishing, 2022, p. 36.

[4] 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. 31.

[5] Ibid., para. 36.

PM May proposed in her Florence[6] and Munich Speech,[7] 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*". 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.[8]

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.[9]

The *"Exiting the European Union*" Select Committee report acknowledges the challenges of negotiating an international data protection agreement while stressing its benefits for regulatory harmonisation and business certainty.[10] The alternatives analysed by the Committee are deemed *"unsatisfactory substitutes*" that burden businesses with unnecessary bureaucracy.[11] Therefore, to ensure continuity of data flows in both directions, it is highly desirable to have an agreement beyond adequacy decision. The reason was 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 had 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*".[12] The UK had already accepted Title 7 of the Withdrawal Agreement,[13] 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.[14]

---

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

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

[8] REINKE, G. *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, p. 74.

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

[10] 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.

[11] Ibid., para. 57.

[12] HM Government. May 2018, *Framework for the UK-EU partnership – Data Protection*, presentation prepared by the UK negotiating team, p. 11.

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

[14] 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.

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.[15] If the UK had failed to comply with the GDPR, it would have led to a breach of the UKęs obligations as a Member State during that period (31 January 2020 – 31 December 2020), which would cause a massive disruption in personal data flows, as the European Commission (the Commission) would likely prohibit transfers from EU Member States to the UK due to such breach.[16]

The UK DPA 2018 was enacted for two interrelated reasons: its legal and economic necessity and the fact that the UK government had not planned for a *"leave*" vote and its consequences before the referendum. Hence, 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.[17]

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.[18] Non-compliance would only increase the burden of data controllers and the business cost for organisations. Hence, the Withdrawal Agreement specified that 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 obtained from any Member State, though the UK had become a third country.[19]

The national implementation of the GDPR into the UK law through the UK DPA 2018 significantly impacted the safeguarding of data subjectsę rights. In its Chapter 12, the UK DPA 2018 shaped the legal basis for safeguarding the rights of EU and UK residents and citizens, covering the key provisions, including special personal data categories,[20] the rights of data subjects,[21] transfers of personal data to third countries,[22] the data protection

[15] 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.

[16] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 38.

[17] 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*").

[18] Article 3 GDPR.

[19] Art 73 of the Withdrawal Agreement, 21 November 2018.

[20] Art 10-11 of the UK DPA 2018.

[21] Art 12-14, 43-54 and 92-100 of the UK DPA 2018.

[22] Article 18 of the UK DPA 2018.

principles,[23] security of data processing,[24] data breach notification,[25] and transfer of personal data to third countries.[26]

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.[27] This solution was welcomed by many data protection experts because *"it could only have the effect of making transfers easier*".[28] 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.[29]

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*." [30]

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 it to attend EDPB meetings (by invitation) but not to vote during this period.[31]

## III. THE UK'S INITIAL APPROACH OF EXCEPTIONALISM

When reviewing its options, the Sub-Committee in charge of the post-Brexit data protection framework considered whether post-transition EEA-UK data flows would be best fa-

[23] Art 34-42 and 85-91 of the UK DPA 2018.
[24] Art 66,107 of the UK DPA 2018.
[25] Art 67-68, 108 of the UK DPA 2018.
[26] Art 72-78, 109 of the UK DPA 2018.
[27] Art 71 (a) and (b) Withdrawal Agreement, 21 November 2018.
[28] BAINES J., DE REYA M. quoted in CLARK, S. No SCCs needed for data controllers governed by GDPR, ICO lawyer suggests. *Global Data Review Blog*. 2018. In: *Lexology* [online]. 12. 10. 2018 [2023-11-03]. Available at: <https://globaldatareview.com/article/no-sccs-needed-data-controllers-governed-gdpr-ico-lawyer-suggests>.
[29] CYBERMATRON. *Data protection in the EU-UK Withdrawal Agreement - Are we being framed?* In: *Cybermatron Blog* [online]. 15. 11. 2018 [2023-11-18]. Available at: <https://cybermatron.blogspot.com/2018/11/data-protection-in-eu-uk-withdrawal.html>.
[30] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 39.
[31] Article 70 and 128(5) of the Withdrawal Agreement, 21 November 2018.

cilitated by seeking either a partial or whole country adequacy decision from the European Commission.[32] In addition, the Sub-Committee discussed alternative solutions 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.[33]

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 EUęs data protection rules and to further promote the UKęs independence as a sovereign country. Brexit was powered by the people's 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*"[34] and *"CJEU judgments on data protection issues hobble the growth of internet companies,"*[35] 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. The UK would also have to accept the authority of the European Data Protection Board as a "rule maker", meaning that the UK would have to accept the EDPB's decision without representation on the Board. This would likely be uncomfortable for those who see Brexit as a complete divorce from the EU institutions.[36] And if the UK did not accept any EDPB decision, it could 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 Commission 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.[37] 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 conces-

[32] Art 45(3) and 93(2) GDPR.

[33] House of Lords. European Union Committee, *Brexit: the EU data protection package*, Paper 7, Chapter 3, paras 112–115.

[34] WHITE, M. Why John Whittingdale is politically tone deaf and 30 years out of date. In: *The Guardian Blog* [online]. 9. 3. 2016 [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>.

[35] GOVE, M. Why I'm backing Brexit. In: *The Spectator* [online]. 20. 2. 2016 [2023-11-18]. Available at: <https://www.spectator.co.uk/article/michael-gove-why-i-m-backing-brexit/>.

[36] MURRAY, A. Data transfers between the EU and UK post Brexit? *International Data Privacy Law.* 2017, Vol. 7, No. 3, p. 151.

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

sion 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*".[38]

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.[39]

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.[40]

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.[41]

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.[42] Instead, it advocates that trade negotiations and adequacy requests be separate but parallel.[43]

---

[38] KUNER, C. *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, O. *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, V., DE HERT, P. The PNR Agreement And Transatlantic Anti-Terrorism Co-Operation: No Firm Human Rights Framework On Either Side Of The Atlantic. *CML Rev.* 2009, Vol. 46, No. 3, pp. 885–919, EUROPEAN PARLIAMENT. *LIBE Committee, Briefing: Personal data protection achievements during the legislative term 2014–2019: the role of the European Parliament.* In: *European Parliament* [online]. April 2019 [2023-11-22]. Availableat: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/608870/IPOL_BRI(2019)608870_EN.pdf>.

[39] DexEU. *The exchange and protection of personal data - a future partnership paper.* In: *HM Government* [online]. 24. 8. 2017 [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>.

[40] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics.* p. 44.

[41] DexEU. *The exchange and protection of personal data - a future partnership paper.* In: HM Government [online]. 24. 8. 2017 [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>.

[42] Letter on cross-border data flows and EU trade agreements. In: *Council of the European Union* [online]. 1. 3. 2018 [2023-11-18]. Available at: <http://data.consilium.europa.eu/doc/document/ST-6687-2018-INIT/en/pdf >.

[43] *EU horizontal provisions on Cross-border data flows and protection of personal data and privacy in the Digital Trade Title of EU trade agreements.* In: *European Commission* [online]. [2023-11-18]. Available at: <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_1462>.

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.*"[44]

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 an assessment to make sure we meet the basic equivalence test set out in the GDPR,"*[45] but neglected to specify how any disputes would be resolved. To no surprise, it was once again rejected with Barnieręs 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.[46] 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. [47]

The Commissionęs 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.[48]

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 Commission. The EU agreed to make an adequacy assessment during the UKęs transition period *"if the applicable conditions are met,"*[49] 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',[50] particularly as *"For the EU, privacy is not a commodity to be traded. Data*

[44] Speech by Michel Barnier at Business Europe Day 2018, Brussels, p. 8. In: *European Commission* [online]. 1. 3. 2018 [2023-11-18]. Available at: <http://europa.eu/rapid/press-release_SPEECH-18-1462_en.html>.
[45] HM GOVERNMENT. *Framework for the UK-EU partnership Data protection.*25 May 2018, pp. 16–17.
[46] Speech by Michel Barnier at the 28th Congress of the International Federation for European Law (FIDE), Lisbon, 26 May 2018, SPEECH/18/3962. In: *European Commission* [online]. [2023-11-18]. Available at: <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_18_3962>.
[47] Ibid.
[48] 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). In: *parliament.uk* [online]. [2023-11-18]. Available at: <https://publications.parliament.uk/pa/cm201719/cmselect/cmexeu/1564/156402.htm>, para 9.
[49] 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.

*protection is a fundamental right in the EU*"[51] and protection of fundamental rights is non-negotiable.[52]

The UK's application for an adequacy decision makes an example of a situation where the context of the adequacy decision often comes 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"*[53] 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.[54]

## IV. THE TCA AND THE TRANSITIONAL DATA PROTECTION ARRANGEMENTS

The Trade and Cooperation Agreement (the TCA) was concluded on Christmas Eve 2020, after ten rounds of negotiations during an eight-month period. 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.[55] 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.[56] 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.[57] 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.[58]

[50] HANKE VELA, J., PLUCINSKA, J., VON DER BURCHARD, H. EU trade, the Martin Selmayr Way. *Politico*. 2017.
[51] Ibid.
[52] FONTANELLA-KHAN, J. Data protection ruled out of EU-US trade talks. *Financial Times*. 2013.
[53] BRADFORD, A. *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press, 2019, p. 14.
[54] Ibid., p. 3.
[55] CELESTE, E. Cross-border data protection after Brexit. *DCU Brexit Institute Working Paper Series*. 2021, No. 4, p. 6.
[56] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 46.
[57] Art COMPROV. 19, TCA.
[58] The provision is to be reviewed in three years; Art 6, TCA.

The TCA itself does not include an adequacy decision to facilitate EEU-UK personal data transfers, as it is a separate process. 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.[59] 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.[60] 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.[61]

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.[62]

The only changes allowed were to align with EU rules, like recognizing new Standard Contractual Clauses (SCC) adopted by the EU.[63] 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.[64]

## V. 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

[59] 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.

[60] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics.* p. 48.

[61] Art FINPROV.10A (1) and (2), TCA.

[62] Art FINPROV.10A (3), TCA; DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics.* p. 49.

[63] Data Protection -Standard Contractual Clauses for Transferring Personal Data to Non-EU Countries (Implementing Act), (Have your say). In: European Commission [online]. [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>.

[64] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics.* p. 49.

GDPR and elaborated on in the EDPB's *"adequacy referential,"* [65] and corresponding CJEU case law.[66]

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.[67] 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.[68]

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 BCRs holder is required to transfer to the appropriate lead authority and appoint a representative, in the relevant jurisdictions.[69]

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.[70]

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.[71] 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.[72] The

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

[66] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 53.

[67] 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.

[68] 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.

[69] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 50.

[70] Ibid.

[71] Section 17A, UK DPA 2018.

[72] 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.

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.[73]

## VI. AN "UNSTABLE" ADEQUACY DECISION

To grant the UK an 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.[74]

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 scrutinise 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*",[75] 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.[76]

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 Charter of Fundamental Rights of the European Union in UK law. Declarations of an intention to "opt-out" of parts of the European Convention on Human Rights (the ECHR), or at least from interpretations of the Convention by the European Court of Human Rights (the ECtHR),[77] 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.[78] Relatedly, the UK's membership in the Five Eyes Intelligence Sharing Alliance presented challenges related to transferring

[73] Section 182(2) of the UK DPA 2018; Art 36(4) of the UK GDPR.

[74] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 51.

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

[76] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 51.

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

[78] BROWN, I., KORFF, D. The inadequacy of UK data protection law Part One: General inadequacy. In: *ianbrown.tech* [online]. [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.

data from EEA countries to the United States or other third countries without an adequacy decision.[79]

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[80] 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.[81]

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.[82]

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.[83] The Commission has, however, indicated a willingness to reassess this exclu-

[79] BROWN, I., KORFF, D. *The inadequacy of UK data protection law Part One: General inadequacy*; DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 51.

[80] 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.

[81] DOUWE, K. The inadequacy of the EU Commission's Draft GDPR Adequacy Decision on the UK. In: *ianbrown.tech* [online]. [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/>.

[82] 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. In: *The European Data Protection Board* [online]. [2023-11-23]. Available at: <https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en>.

[83] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 53.

sion once it has been remedied under UK law.[84] 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 data collection by UK intelligence authorities is limited to what is strictly necessary to achieve the legitimate objective in question.[85] 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.[86]

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.[87] 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.[88]

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.[89] The UK's inconsistent stance on the European Convention on Human Rights has not gone unnoticed by the Commission,[90] 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*".[91] It is clear that withdrawal from the European Convention on 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

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

[85] 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.

[86] DOUWE, K. *The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK*; MANANCOURT, V., UK data flows get Brussels' blessing, with caveats. In: *Politico* [online]. 17. 4. 2021 [2023-11-03]. Available at: <https://www.politico.eu/article/uk-privacy-data-flows-europe-blessing-caveats/>.

[87] 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, pp. 8–9.

[88] 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.

[89] European Commission. Press Release: Data protection: Commission adopts adequacy decisions for the UK. In: *European Commission* [online]. 28. 6. 2021 [2023-11-18]. Available at: <https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3183>.

[90] BOWCOTT, O. *UK government plans to remove key human rights protections.*

[91] European Commission. Press Release: Data protection: European Commission launches process on personal data flows to the UK. In: *European Commission* [online]. 19. 2. 2021 [2023-11-18]. Available at: <https://ec.europa.eu/commission/presscorner/detail/en/IP_21_661>.

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.[92]

## VII. THE FUTURE OF UK'S ADEQUACY

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.[93]

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*",[94] 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.[95]

The prospect of the UKęs 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.[96]

Again, constraints and dependencies have led some to question whether the UK should pursue regulatory divergence in the longer term. 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.[97]

---

[92] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics.* p. 54.

[93] CELESTE, E. Cross-border data protection after Brexit. *DCU Brexit Institute Working Paper.* 2021, Series, No 4, p. 12.

[94] 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. In: *International Commissioneręs Office* [online]. [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/>.

[95] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics.* p. 55.

[96] Ibid.

[97] The Taskforce on Innovation, Growth and Regulatory Reform (TIGRR), pp. 49–53. Independent Report. In: *The Taskforce on Innovation, Growth and Regulatory Reform* [online]. 16. 6. 2021 [2023-11-23]. Available at: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/994125/FINAL_TIGRR_REPORT__1_.pdf>.

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)"*,[98] a concern that was also identified in the UK National Data Strategy.[99] Axel Voss, MEP, one of the strongest advocates of the GDPR has also asserted that *"the GDPR is not made for blockchain, facial or voice recognition, text and data mining [. . .] artificial intelligence*".[100] He argues that the GDPR, *"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."*[101]

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.[102] 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.[103]

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.[104] 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.[105]

---

[98] 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. In: *European Commission* [online]. 24. 6. 2020 [2023-11-23]. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264>.

[99] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 59.

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

[101] VOSS, A. How to bring GDPR into the digital age. In: *Politico* [online]. 25. 3. 2021 [2023-11-24]. Available at: <https://www.politico.eu/article/gdpr-reform-digital-innovation/>.

[102] 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.

[103] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 57.

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

[105] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 58.

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 as it is important to mention that the Convention 108+ offers rather a baseline level of protection rather than the comprehensive and strict framework offered by the GDPR, outlining fundamental principles and absenting strong data protection enforcement mechanisms This option could be considered since the UK has already ratified Convention 108+. However, doing so would 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.[106]

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.[107]

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.

## CONCLUSION

In terms of personal data protection, Brexit was 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 extra-territorial application of the UK and EU GDPR, companies established in one jurisdiction that offer goods and services or monitor the behaviour of data subjects in another jurisdiction must comply with both laws.[108] 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.[109]

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

[106] Ibid., p. 59.
[107] 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.
[108] CELESTE, E. *Cross-border data protection after Brexit.* p. 12.
[109] Ibid.

should not be taken for granted. On the contrary, it must remain fit for purpose.[110] 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".[111]

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 did 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.[112]

[110] DE HERT, P., GONZALEZ-FUSTER, G., VAN BRAKEL, R. *Research handbook on privacy and data protection law: values, norms and global politics*. p. 57.
[111] Ibid., p. 60.
[112] CELESTE, E. *Cross-border data protection after Brexit*. p. 12.