2. Post-Brexit data protection in the UK – leaving the EU but not EU data protection law behind[1]

Karen McCullagh

1. INTRODUCTION

On 31 January 2020 the United Kingdom (UK) formally left the European Union (EU) after 47 years of membership, following the outcome of the historic 'Brexit' referendum on 23 June 2016 in which a majority of eligible voters in the UK voted to 'Leave' the EU.[2] As the decision to leave the EU (the world's largest trading bloc[3] and the UK's largest trading partner)[4] was momentous one might have expected the UK government to have engaged in contingency planning and to have decided on the nature and degree of future trading relationship it would seek with the EU and other countries prior to the referendum but the UK government did not take these actions because it did not expect the 'leave' vote to win the referendum.

Consequently, it was unprepared for the outcome and a great deal of political turmoil ensued – including the resignation of two prime ministers, and the UK requesting postponement of its departure from the EU on three occasions in the next three years because of disagreements amongst UK government ministers over the scope and terms of the withdrawal agreement, – before the EU and UK eventually agreed the terms of a Trade and Cooperation Agreement on 24 December 2020, a mere seven days before the UK would have 'crashed out' of the EU on a 'no deal' basis.

The government's failure to plan for Brexit included a failure to give any thought to data protection arrangements, that is, whether it would continue to comply with EU data protection law as it had since Directive 95/46/EC came into force, or whether it would seek to diverge

[1] The author thanks Mr Jon Baines, Mr Neil Brown, Prof Morten Hviid, Prof David Mead, Mr Daragh O'Brien, Dr Katherine O'Keefe, Prof Claudina Richards, and the anonymous reviewer for their comments on earlier drafts.

[2] Brexit is a neologism of British and Exit coined in 2012 by Peter Wilding which expresses the UK's withdrawal from the EU; http://ww w .bbc .com/ culture/story / 20190314 -how -brexit -changed -the -english -language accessed 19 April 2021; Brexit is the outcome of a referendum held on 23 June 2016 across the UK and Gibraltar about whether or not the UK should remain a member of the EU. A majority of eligible voters (17.41 million people; 51.9 per cent of all voters) voted to leave the EU; Electoral Commission, 2016, EU referendum results, https://ww w .electoralcommission .org .uk/ find -information -by -subject/ elections -and -referendums/ past -elections -and -referendums/ eu -referendum/ electorate -and -count -information accessed 19 April 2021; Prime Minister's Office, Prime Minister's letter to Donald Tusk triggering Art 50, 29 March 2017, https://ww w .gov .uk/ government/ uploads/ system/ uploads/ attachment _data/ file/ 604079/ Prime _Ministers _letter _to _European _Council _President _Donald _Tusk .pdf accessed 19 April 2021.

[3] European Commission, 'EU position in world trade,' 9 February 2019, https://e c .europa .eu/ trade/ policy/e u -position -in -world -trade/inde x _en .htm accessed 19 April 202.1

[4] House of Commons Library,' Research Briefing: Statistics on UK-EU trade,' 10 November 2020 https://commonslibrar y.parliamen t.uk / research -briefings/cb p -7851/ accessed 19 April 2021.

either in the immediate or longer term. Accordingly, the objective of this chapter is to trace how the UK data protection framework evolved from the time of the Brexit referendum to the adoption by the Commission of an EU-UK adequacy decision, and to explain why the UK has, for the time being, decided not to diverge from EU data protection law.

The chapter begins by explaining why the UK decided to comply with the GDPR before becoming a third country for EU data protection purposes and then illustrates that the Brussels effect, that is, 'multinational companies voluntarily extend[ing] the EU rule to govern their global operations',[5] influenced the UK's decision to continue to comply with EU data protection standards after it became a third country. It also discusses why the UK initially sought to pursue an exceptionalism strategy – seeking a bespoke data agreement outside the scope of the GDPR adequacy framework before eventually conceding that it would need to seek an adequacy decision from the European Commission (the Commission) to facilitate EEA-UK personal data transfers. Thereafter, it demonstrates that although the UK has secured an adequacy decision it may prove unstable. Finally, it considers whether longer-term divergence is likely or not and concludes that whilst a degree of friction and divergence is likely, multi-national data controllers are unlikely to call for the UK government to completely diverge from the GDPR if it continues to meet their needs because divergence would result in further compliance burdens which would be an unwelcome business cost. Therefore, EU data protection advocates have rightly framed the UK's continued compliance with the GDPR as early evidence of the EU's ability, through its trade and regulatory power, to 'export' its laws and standards to third countries by offering unrestricted access to its large and valuable marketplace of personal data in return for confirmation of legal compliance, via an adequacy assessment.[6] However, for the EU to be assured that the GDPR standards become and remain the global norm, it must ensure that it remains fit for purpose, which is why it is trite to say that the UK has left the EU but not EU data protection law behind, for now, at least.

2. DATA PROTECTION DURING THE NEGOTIATION PERIOD (2016–2020)

The UK government knew that the GDPR would supersede Directive 95/46/EC and be directly applicable in all EU member states and EEA countries, including the UK, from 25 May 2018 until the end the transition period on 31 December 2020.[7][8] Failure to give effect to and to fully comply with the GDPR would have left the UK in breach of its member state obligations during that period (31 January 2020 – 31 December 2020) and could have led to disruption in personal

[5] Anu Bradford, *The Brussels Effect: How the European Union Rules the World*, (OUP, 2012), XIV.

[6] A. Bendiek and M. Römer, M. (2019) 21(1) 'Externalizing Europe: the global effects of European data protection' (2019) *Digital Policy, Regulation and Governance* 32-43, 33 and 35; Patrick Müller and Gerda Falkner 'The EU as a policy exporter? The conceptual framework', in Gerda Falk ner and Patrick Müller (eds), *EU Policies in a Global Perspective: Shaping or Taking International Regimes?* (London: Routledge, 2014), 11–12.

[7] 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, a text with EEA relevance, into the EEA Agreement, and it entered into force in all three EFTA-EEA States on 20 July 2018; Decision of the EEA Joint Committee, No [8] /2018, OJ No L 183/23, 19.7.2018,

data flows if the Commission prohibited transfers from EU member states to the UK.[9] It therefore enacted the Data Protection Act 2018, (hereafter DPA 2018) to repeal and replace the Data Protection Act 1998 and give effect to national derogations permitted by the GDPR before exit from the EU on 31 January 2020, and during the transition period for two inter-related reasons,[10] the first of which was legal and economic necessity.

A second reason for maintaining compliance with the GDPR during the transition period was that the UK government had not planned for a 'leave' vote and attendant consequences before the referendum, so it did not have an alternative ready to 'roll out'. The easiest option, therefore, was to maintain the status quo until it had evaluated the merits of diverging from the GDPR which was hailed as a clarion call for a new global digital gold standard of data protection,[11] particularly as the GDPR would continue to have extra-territorial application to UK data controllers offering goods or services to individuals or monitoring the behaviour of individuals in EEA countries, thereby necessitating ongoing compliance with the GDPR.[12] Divergence before then would merely have increased the compliance burden of data controllers and been an unwelcome business cost.

The Withdrawal Agreement therefore specified that the GDPR would continue to apply (with the exception of Chapter VII – co-operation & consistency) in the UK during the transition period (31 Jan 2020 – 31 December 2020) in relation to personal data transferred between the EEA and the UK[13] and that data received from the UK would not be treated differently to data received from EU member states even though the UK had left the EU.[14] In essence, it created a 'GDPR-envelope' that applied to personal data processed in the UK during the transition period, and would continue to be processed in the UK in reliance of these arrangements after the transition period ended thereby ensuring that 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.[15]

Confirmation that UK-based data controllers and processors could continue to receive personal data from EEA countries during the transition period without needing to put in place Chapter V transfer mechanisms (e.g., model clauses or binding corporate rules, or rely one of the derogations) was welcomed by many data protection experts because 'it could only have the effect of making transfers easier'.[16] However, a few data protection experts reacted with

---

[9] Art 45, Recital 107 GDPR It could, subject to an infringement action by the Commission, eventually result pecuniary sanctions (Arts 258 and& 260 TFEU) but the Commission might decide not to pursue this course of action in respect of the UK because it is a lengthy and time-consuming process – one that might prove futile in respect of a member state in the process of exiting the EU.

[10] For a detailed analysis of the national derogations to the GDPR in the Data Protection Act 2018 see: Karen Mc Cullagh, 'The UK Data Protection Act 2018,' E-Conference on National Adaptations to the GDPR, (*Blogdroiteuropéen*, 4-6 June 2018), https://blogdroiteuropee n .files .wordpress .com/2018 / 06/ karen .pdf accessed 19 April 2021.

[11] EDPS, The EU GDPR as a clarion call for a new global digital gold standard, 1 April 2016, https:// edps .europa .eu/ press -publications/ press -news/ blog/ eu -gdpr -clarion -call -new -global -digital -gold -standard _en accessed 19 April 2021; The DPA 2018 provides for two separate regimes for general processing: one for processing that falls within the scope of the GDPR and a separate, broadly equivalent regime for processing that falls outside the scope of the GDPR (the 'applied GDPR').

[12] Art 3 GDPR 2016/679.

[13] Arts 71 and Art 127.

[14] Art 73.

[15] Art 71 (a) and (b)

[16] Jon Baines, Mischon de Reya, quoted in Sam Clark, 'No SCCs needed for data controllers governed by GDPR, ICO lawyer suggests,' (*Global Data Review Blog* 12 October 2018), https://globaldatarevie

concern to the 'GDPR-envelope' because it would allow the UK to temporarily avoid compliance with the *Schrems* criteria i.e., fundamental rights limitations on surveillance.[17] In my view, drafting and implementation of Chapter V compliance measures e.g., contractual arrangements would have been a costly, time-consuming, and onerous exercise that would have unfairly penalised small- and medium-sized enterprises, causing harm to both the EU and UK economies, which both parties were keen to avoid, particularly as an adequacy decision could well be in place before the other mechanisms were finalised. The pragmatic 'fudge' minimised economic harm by ensuring that EEA/EU-UK personal data transfers continued unimpeded during the transition period.

In the interests of seamless continuity, the Withdrawal Agreement stipulated that the CJEU would have jurisdiction to settle questions of interpretation raised by the UK courts regarding data protection law and the UK would abide by CJEU decisions during the transition period. Likewise, 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. As such, they were able to continue to designate the UK national supervisory authority, the Information Commissioner's Office (ICO), as their lead supervisory authority to coordinate actions and complaints regarding cross-border processing (e.g., a complaint originating in France or Germany), with the help of other 'concerned DPAs' (i.e., other data protection authorities in member states affected by the processing), thereby minimising the administrative burden of compliance.

However, as Chapter VII of the GDPR did not apply under the terms of the Withdrawal Agreement the ICO ceased to be a full member with voting rights of the European Data Protection Board (EDPB), as of 31st January 2020. Instead, the ICO had 'observer' status, that is, it was permitted to attend (by invitation) but could vote in meetings of the EDPB during this period.[18]

3. DIVERGENCE V CONTINUED ALIGNMENT: THE BRUSSELS EFFECT?

As alluded to above, the UK government did not have an agreed vision about the nature or extent of the trade deal it wished to secure with the EU or other countries when it triggered Article 50, to commence the process of leaving the EU.[19] Nor did it have an agreed vision regarding data protection.

One might have expected the UK government to immediately declare an intention to maintain compliance with EU data protection laws given that this would ensure that the UK provides an essentially equivalent level of protection and increase the likelihood of securing and thereafter retaining an adequacy decision to facilitate personal data-enabled services

w .com/ data -privacy/n o -sccs -needed- data- controllers- governed -gdpr -ico -lawyer -suggests accessed 19 April 2021.

[17] Cybermatron, Data protection in the EU-UK Withdrawal Agreement - Are we being framed?, (*Cybermatron Blog*, 15 November 2018) http://cybermatro n .blogspot .com/ 2018/ 11/ data- protection-in -eu -uk -withdrawal .html accessed 19 April 2021.

[18] Arts 70 and 128(5).

[19] The UK Prime Minister invoked Art 50 of the Treaty on European Union (TEU) which commenced the UK's withdrawal, commonly known as Brexit, from the EU; Prime Minister's Office, Prime

exports from the EU to the UK – they were worth approximately £42bn (€47bn) whilst exports from the UK to the EU were worth £85bn (€96bn) in 2018.[19] However, there were calls for Brexit to be used as an opportunity to diverge from the EU standard by those who viewed the GDPR standards as being too high[20] and contended that lower, less onerous standards would give the UK leverage when engaging in trade deals with other countries.[21]

The House of Lords EU Home Affairs Sub-Committee considered how the UK government might meet its objective of ensuring 'unhindered and uninterrupted data flows with the EU' and facilitating transfers to non-EEA countries e.g., the US. It heard evidence that the UK and EU economies are currently very heavily integrated – three-quarters of the UK's cross-border data flows are with EU countries – and forecast to remain so for decades to come. Business representatives were particularly cognisant of the trade power of the EU. For example, Antony Walker of TechUK emphasised that 'we have to remember the size of the UK market versus the size of the European market',[22] which means that 'we will have to do that very much in partnership with the European Union, rather than simply boldly striking out by ourselves and hoping others will follow'.[23] Business representatives also made implicit mention of the Brussels effect, that is, the regulatory 'race to the top' whereby the most stringent standard has an appeal to companies operating across multiple regulatory environments as it makes global production and exports easier.[24]

> If you are running [a] global operation, you will want to have consistent processes across your businesses. What we are seeing is that global firms based outside of the EU are taking the GDPR as the norm for their business and are building their processes around it, so, for very large companies, there is no desire to diverge from the GDPR—the opposite, because they worry about falling between the gaps.[25]

In short, the Sub-Committee was advised that there was little appetite in the business sector for wholescale divergence from the EU data protection standard.

Minister's letter to Donald Tusk triggering Art 50, 29 March 2017, https://ww w .gov .uk/ government/ uploads/ system/ uploads/ attachment _data/ file/ 604079/ Prime _Ministers _letter _to _European _Council _President _Donald _Tusk .pdf accessed 19 April 2021.

[19] Estimated by the UK government's Department for Digital, Culture, Media and Sport by applying the UN definition of digitally deliverable services (DDS) to UK Office for National Statistics data; cited in DCMS, Explanatory Framework for Adequacy Discussions, Section A: Cover Note, 13 March 2020,
1.

[20] Federation of Small Businesses, 'Manifesto European Elections 2014' (February 2014).

[21] Daniel Castro, 'Brexit Allows UK to Unshackle Itself from EU's Cumbersome Data Protection Rules', (Centre for Data Innovation, 20 July 2016) https://ww w .datainnovation.org / 2016/ 07/brexi t - allows- uk- to -unshackle- itself -from -eus -cumbersome- data- protection- rules/ accessed 19 April 2021.

[22] Ibid., para 129.

[23] Ibid.

[24] Anu Bradford, The Brussels effect,' (2012) *NW U Law Rev*, 107(1), 1–68, 9.

[25] House of Lords, European Union Committee, 'Brexit: the EU data protection package,' 3rd Report of Session 2017–19 - published 18 July 2017 – HL Paper 7, para 128.

Evidently the EU is able, through its '*trade power*,' to 'export' its laws and standards to other countries by offering improved access to its large and valuable market in return for legal

compliance.[20] And, the UK's application for an adequacy decision exemplifies that an adequacy decision is often made in the context of an asymmetrical power relationship, with the EU wielding significantly more economic power than the third country, and this dynamic allows the EU to *de facto* impose its legislative framework onto a third country which is seeking to strengthen or, in the case of the UK, dependent upon and seeking to maintain strong economic ties with the EU. The 'behaviour of market actors' also drives this externalisation of EU regulatory policy, an impact Bradford labelled the 'Brussels effect' when describing the EU's 'unilateral regulatory globalisation', that is, the extension of EU regulatory norms and practices beyond the EU territory but outside the structures and institutions of hierarchical public rule-making.[21] As Bradford and Walker have highlighted, multinational corporations are obliged to comply with the GDPR to gain access to the EU market, and as these multinational companies prefer to deal with as few legislative frameworks as possible, they promote through compliance with it, the GDPR as the global regulatory standard, not least to avoid the additional costs of compliance with multiple rules and to gain the economies of scale achieved by promoting compliance with the GDPR. Consequently, trade and market forces were drivers of the UK's continued compliance with EU data protection law, post Brexit.

3.1 Bespoke Data Agreement v Mutual Adequacy Decisions

The Sub-Committee was further advised that the UK, as a third country, would not benefit from *de jure* recognition of its data protection laws as providing an adequate standard of protection to facilitate EEA-UK personal data transfers, and it therefore considered alternative mechanisms for effectuating such transfers.[22] Specifically, it considered whether post-transition EEA-UK data flows would be best facilitated by either seeking either a partial adequacy decision or a whole country adequacy decision from the European Commission.[23] The Committee also considered, in the alternative, the merits of requiring individual data controllers and processors to adopt their own compliance measures such as model clauses or binding corporate rules.

Expert witnesses confirmed that the UK-established data controllers favoured a whole country (as opposed to sectoral) adequacy decision and continued harmonisation with the EU data protection framework because it would be the 'least burdensome' option and offer 'stability and certainty for businesses', particularly small- and medium-sized UK-based data controllers and processors that could not easily absorb the legal costs associated with drafting and obtaining approval for model clauses or other legal mechanisms to effectuate transfers.[24] It also reported that if the UK were to obtain an adequacy decision from the Commission to facilitate EEA-UK personal data transfers it would have regulatory implications for data transfer agreements between the UK and other third countries because compliance with the

[20] Bendiek and Röme (n 8); Müller and Gerda (n 8), 11–12.

[21] Bradford (n 28), 3.

[22] Art 45, GDPR.

[23] An (whole country) adequacy decision confirm with binding effects on EEA countries that the level of data protection in the UK is 'essentially equivalent' to that in EU member states such that additional safeguards would not be required nor would UK-based data controllers in be required to individually show compliance with the GDPR to facilitate transfers of personal data from EEA countries to the UK, whereas a partial or sectoral adequacy decision applies only to a particular sector e.g., the commercial sector. See Arts 45(3) and 93(2) of the GDPR for further information on implementing acts.

[24] House of Lords, European Union Committee, 'Brexit: the EU data protection package (n 29), Paper 7, Chapter 3, paras 112–115.

onward transfer principle in the GDPR would necessitate restrictions on transfers of personal data of individuals in EEA countries from the UK to countries that do not meet EU data protection standards.

Whilst the Sub-Committee rightly focused on economic considerations, the government also had to give due weight to political considerations to build and maintain government support for the trade negotiations so that Parliament would ratify any deal reached. Some Brexiteers had, in the run up to the Brexit referendum, claimed Brexit would offer a unique opportunity to restore sovereignty by 'freeing' the UK from EU laws and institutions and data protection framework, and that this would be beneficial because 'the EU had imposed data protection requirements' which are 'against British interests',[25] and 'ECJ [European Court of Justice] judgments on data protection issues hobble the growth of internet companies',[26] and were therefore loath to accept EU institutions having any continuing jurisdiction.

In this regard, an adequacy decision would be an anathema as it would necessitate the UK accepting oversight by various EU institutions, for instance, the Commission having the ability to withdraw an adequacy decision, and member states' national data protection authorities having the power to order the suspension of data flows to the UK. The UK would also have to accept the jurisdiction of the European Data Protection Board as a 'rule-taker', that is, the UK would have to accept decisions of the EDPB without representation on the Board, a position likely to be quite unpalatable to those who view Brexit as a complete divorce from EU institutions.[27] And should the UK fail to accept any decision of the EDPB, it may lose its adequacy status. Relatedly, the UK would also have to accept indirect oversight roles by the Council and Parliament because these bodies may at any time request that the Commission amend or withdraw an adequacy decision on the grounds that its enactment exceeds the implementing powers provided for in the GDPR.[28] Moreover, as the EU is an autonomous legal order, any EU-UK adequacy decision made by the Commission could be subject to challenge before the CJEU which holds itself out as the guardian of fundamental rights.[29] Acceptance of

[25] Michael White, 'Why John Whittingdale is politically tone deaf and 30 years out of date,' (*The Guardian Blog*, 9 March 2016), https:// www .theguardian .com/ politics/blog /2016 / mar/09 / why -john -whittingdale- is- politically- tone- deaf- and-3 0 -years- out- of- date accessed 19 April 2021.

[26] Michael Gove, 'Why I'm backing Brexit,' (*The Spectator,* 20 February 2016), <https://ww w .spectator.c o.uk / article/michae l- gove -why- i- m -backing- brexit accessed 19 April 2021.

[27] Andrew Murray, 'Data transfers between the EU and UK post Brexit?,' (2017) *International Data Privacy Law*, 7 (3), 149–164, 151.

[28] European Commission, 'How the EU determines if a non-EU country has an adequate level of data protection,' https://e c .europa .eu/ info/ law/ law -topic/dat a -protection/internationa l- dimension -data -protection/adequac y- decisions _en accessed 19 April 2021; For example, a non-binding resolution by the Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) of the European Parliament that the Commission suspend the EU-US. Privacy Shield unless and until corrective actions were taken by the US Department of Commerce prompted amendments to the operation of the Privacy shield before a second annual review of the scheme by the Commission.

[29] *Schrems* and *Opinion 1/15* confirm that if the Commission were to enter into an EU-UK adequacy agreement on terms contrary to primary law, including the Charter, then it could be struck down by the ECJ. For a discussion of the crucial role of the CJEU both in negotiating international agreements and in developing the European model of personal data protection and respect for private life. See, Christopher Kuner, 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; Olivia Tambou, 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; Vagelis Papakonstantinou and Paul De Hert, 'The PNR Agreement And Transatlantic Anti-Terrorism

this oversight role would represent a major concession by the UK government as it had made ending the jurisdiction of the CJEU a 'red line' issue in early statements on the UK's withdrawal from the EU.[30]

Efforts to reconcile conflict between the UK's economic and political objectives led the UK government to initially pursue a strategy of exceptionalism. It proposed that the UK should receive preferential treatment in the form of a free trade deal with the EU and close cooperation on inter alia law enforcement and criminal justice matters and on security and defence matters, with mutual recognition of each other's data protection laws in the absence of an adequacy assessment.[31] The UK further proposed to deal with data protection disputes through provisions in the trade and cooperation agreement, should one be agreed, instead of the GDPR oversight and enforcement mechanisms; the underlying motivations were to prevent the EU from having the power to unilaterally rescind an adequacy decision thereby immediately halting EU-UK data transfers should the UK be found to be substantially in breach of the GDPR. Various factors were cited in support of these bespoke proposals including compliance with EU data protection laws during the transition period and retention of the GDPR in UK law thereafter.[32]

The exceptionalism approach was roundly and repeatedly rejected by the EU for several reasons, not least because construction of the single market has been accomplished not only through the elimination of barriers to the flow of capital, goods, services and labour, but also by the development of a legal order and corresponding range of measures to regulate economic activity within and across borders, including the GDPR, which regulates data protection in all member states.[33] If the Commission unilaterally agreed to a bespoke data agreement with weaker obligations it could give a third country a competitive trade advantage, and ultimately undermine the single market itself. Accordingly, although the Commission has drafted 'non-negotiable horizontal provisions for cross-border data flows and for personal data protection' for inclusion in trade agreements with the aim of reducing barriers to trade, such as forced data localisation in a state's territory, it envisages only using them in situations where under the data protection track an adequacy decision cannot be realistically adopted,[34] and instead advocates that trade negotiations and applications for an adequacy assessment follow separate but parallel tracks.[35] This approach allows the EU to achieve its goal of promoting the GDPR

Co-Operation: No Firm Human Rights Framework On Either Side Of The Atlantic,' (2009) *CML Rev*, 46(3) 885–919.

[30] European Parliament, LIBE Committee, Briefing: Personal data protection achievements during the legislative term 2014–2019: the role of the European Parliament, April 2019, https://ww w .europarl .europa .eu/ RegData/etudes / BRIE/ 2019/ 608870/ IPOL _BRI(2019)608870 _EN .pdf accessed 19 April 2021, 4.

[31] DexEU, The exchange and protection of personal data - a future partnership paper, 24 August 2017, https://asset s .publishing .service.go v .uk/ government/uploads /system /uploads / attachment_data / file/639853 /Th e_exchang e_an d _protection_o f _personal_dat a.pdf accessed 19 April 2021.

[32] Ibid., 8.

[33] Mitchell P. Smith, "Single market, global competition: regulating the European market in a global economy," (2010) *Journal of European Public Policy*, 17(7), 936–953.

[34] European Commission, Letter on cross-border data flows and EU trade agreements, 1 Mar. 2018, http://dat a .consilium.europ a .eu/ doc/document /S T -6687 -2018 -INIT/ en/ pdf; Art 216 (1) TFEU allows authority for the conclusion of an international agreement to be 'provided for in a legally binding Union act', which would allow EU legislation to set out criteria for data protection agreements with third countries; For more information on the inclusion of horizontal clauses in EU trade agreements see: Svetlana Yakovleva and Kristina Irion, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade' *International Data Privacy Law*, (2020).

[35] In 2018 the European Commission endorsed horizontal provisions for inclusion in trade agreements that allow the EU to tackle protectionist practices in third countries in relation to digital trade while

as the global standard, whilst simultaneously ensuring that its integrity and competitiveness is not undermined.

Unsurprisingly, Michel Barnier, the then chief negotiator for the EU, dismissed the UK's proposal for bespoke data protection arrangement saying:

> 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.[36]

Mr Barnier's comments about no system of mutual recognition pre-date a landmark agreement between the EU and Japan to pursue mutual adequacy recognition and must be understood in the context of the UK's proposal for a bespoke adequacy agreement outside the scope of the GDPR adequacy criteria and procedure. His point about an adequacy decision being an autonomous decision remains valid.

The UK government subsequently proposed a new agreement between the EU and UK, that would 'build on a standard adequacy arrangement' and conceded that the Commission would 'conduct an assessment to assure itself that we meet the essential equivalence test provided for in the GDPR'[43] but the UK did not specify how any disputes would be resolved. Unsurprisingly, a few days later, Mr Barnier, once again rejected the UK's proposals. He said that the UK's plans posed 'real problems' and raise a number of legal questions, specifically:

> 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] the UK must understand that the only possibility for the EU to protect personal data is through an adequacy decision.[37]

He insisted that a post-Brexit data protection agreement could not be divorced from the EU's GDPR rules and procedure on adequacy assessment; the UK would have to agree to submit to an adequacy assessment, and by implication, the UK would have to agree to periodic review of an adequacy decision and oversight by the CJEU.

Thereafter, the UK government published a Technical Note on the benefits of a new data protection agreement in which repeated the case for a bespoke legally binding agreement on the basis that:

---

ensuring that trade agreements cannot be used to challenge the high level of protection guaranteed by the EU Charter of Fundamental Rights and the EU legislation on the protection of personal data; European Commission, EU horizontal provisions on *Cross-border data flows and protection of personal data and privacy* in the Digital Trade Title of EU trade agreements, <http:// trade.e c.europ a .eu/ doclib/ docs/ 2018/july /trado c_15713 0.pd f

[36] European Commission, Speech by Michel Barnier at Business Europe Day 2018, Brussels, 1 March 2018, http://europ a .eu/ rapid/pres s- release _SPEECH -18 -1462 _en .htm accessed 19 April 2021, 8.

[43] HMG, Framework for the UK-EU partnership Data protection, 25 May 2018, 16–17.

[37] European Commission, Speech by Michel Barnier at the 28th Congress of the International Federation for European Law (FIDE), Lisbon, 26 May 2018, SPEECH/18/3962, http:// europa .eu/ rapid/ press -release _SPEECH -18 -3962 _en .htm accessed 19 April 2021.

> a key benefit of such an agreement, over a standard Adequacy Decision, is that we can negotiate the right governance mechanisms for our future data relationship. This could include an agreed approach to the standards applied and their interpretation, and to enforcement and dispute resolution.[38]

It proposed to resolve disputes using the terms of a bespoke agreement with the explicit aim of avoiding a *Schrems*-like scenario, that is, the Commission would not be able to unilaterally suspend or repeal an adequacy decision thereby halting EU-UK data transfers. Subsequently, the UK government published a further paper in which it repeated its proposals but added that, 'The UK is ready to begin preliminary discussions on an adequacy assessment so that a data protection agreement is in place by the end of the implementation period at the latest.'[39]

Given the Commission's consistent refusal to offer the UK a bespoke data protection agreement outside the scope of the GDPR adequacy criteria and procedure, the UK's Exiting the EU Committee proposed a pragmatic solution. It 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.[40]

The UK pursued this course of action – the political declaration outlined an intention by the UK to seek an adequacy assessment during the transition period with the EU confirming an intention to adopt an adequacy decision by the end of the transition period 'if the applicable conditions are met',[41] that is, should the UK satisfy the 'essentially equivalent' level of protection test. In effect, the trade negotiations and adequacy assessment were conducted on separate, parallel tracks, something the EU could insist upon as the stronger economic party in the negotiations. The EU insisted on this course of action to ensure that the UK could not seek to lower EU data protection standards during any trade negotiations. The Commission takes the view that they should be kept separate 'to keep trade deals uncontroversial',[42] particularly as 'For the EU, privacy is not a commodity to be traded. Data protection is a fundamental right in the EU'[43] and protection of fundamental rights is non-negotiable.[44] By divorcing the adequacy assessment from trade talks, the EU maintained a strategic competitive advantage while simultaneously defending its own regulatory principles. And it did so, because as Lynskey observes:

---

[38] HM Government, Technical Note: Benefits Of A New Data Protection Agreement, 7 June 2018, https:// assets .publishing .service .gov .uk/ government/ uploads/ system/ uploads/ attachment _data/ file/ 714677/ Data _Protection_Technica l_Not e.pdf accessed 19 April 2021, para 6.

[39] HMG 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) https://publication s.parliamen t.uk / pa/ cm201719/cmselect /cmexeu /1564 / 156402 .htm accessed 19 April 2021, para 3.

[40] Ibid., para 9.

[41] Political declaration setting out the framework for the future relationship between the European Union and the United Kingdom, OJ 2019 C 384 I/02.

[42] Jakob Hanke Vela, Joanna Plucinska and Hans von der Burchard, 'EU trade, the Martin Selmayr way,' (*Politico*, 21 Feb. 2018).

[43] Ibid.

[44] The EU similarly excluded data protection from the remit of the Transatlantic Trade and Investment Partnership (TTIP) negotiations (on a proposed trade agreement between the E U and the US), at least in part because of concerns that the talks would put downward pressure on European standards, something the Commission was been unwilling to countenance; James Fontanella-Khan, 'Data protection ruled out of EU-US trade talks', (*Financial Times*, 4 November 2013); Jakob Hanke Vela, Joanna Plucinska and Hans von der Burchard, 'EU trade, the Martin Selmayr way,' (*Politico*, 21 Feb. 2018).

> in data protection law, although there is no reference to mutual trust in the GDPR or the 1995 Directive, it is the assumed mutual respect for fundamental rights standards (provided for in EU secondary legislation) that facilitates the 'free movement' of personal data within EU Member States, without need for formal adequacy findings.[45]

Such trust does not automatically exist in relation to third countries, rather it must be built through formal legal relationships; and as Lynskey notes, it is this change in status i.e., from trusted member state to third country that explains why 'on the eve of the end of the transition period the UK is de facto "adequate" as an EU Member State while the following day it is not'.[46] The UK applying for and obtaining an adequacy decision would restore that trust.

The need to build trust through a legal mechanism also explains why the Political Declaration further stated that the UK 'will take steps to ensure comparable facilitation of personal data flows to the [European] Union' signalling an intention on the part of the UK to pursue mutual adequacy recognition arrangements.[47] The UK, as sovereign state, is equally entitled to assess the adequacy of protection provided by EU member states and any other country seeking to engage in data transfers with it.

4. THE TRADE AND COOPERATION AGREEMENT

On 24 December 2020, after ten rounds of negotiations during an eight-month period, and a mere seven days before the Transition Period was due to end, after which the UK would have commenced trading with the EU on a 'no-deal' basis, that is on World Trade Organisation terms that would have been very economically damaging for both parties, the UK and EU agreed upon the terms a Trade and Cooperation Agreement (TCA). The TCA was signed by both parties on 30 December 2020. On that date the UK Parliament approved it and it was implemented it into UK law by the enactment of the European Union (Future Relationship) Act 2020. It was applied on a provisional basis within the EU from 1 January 2021 until it entered into force on 1 May 2021 after ratification, by the Council of the EU and the EU Parliament.[48]

While it is less wide-ranging than many had hoped for, it does at least provide a measure of certainty in some respects – not least in relation to the avoidance of tariffs or quotas on goods passing between the UK and the EU. It also provides for limited mutual market access in services (subject to further negotiations on certain aspects e.g., equivalence for financial services), as well as for cooperation mechanisms in a range of policy areas, including data protection and transitional provisions about EU access to UK fisheries, and UK participation in some EU programmes.

---

[45] Orla Lynskey, Extraterritorial Impact in Data Protection Law through an EU Law Lens, *DCU Brexit Institute Working Paper* Series – No 8/2020, 12.

[46] Ibid., 6.

[47] HMG, Political Declaration Setting Out The Framework For The Future Relationship Between The European Union And The United Kingdom, (19th October 2019) https://asset s.publishin g .service .gov .uk/ government/ uploads/ system/uploads /attachmen t_data / file/ 840656/ Political_Declaratio n _setting _out _the _framework _for _the _future _relationship _between _the _European _Union _and _the _United _Kingdom .pdf accessed 19 April 2021.

[48] Art 217 TFEU; The European Parliament voted by a majority of 655 in favour of the TCA on 27 April 2021. On 29 April 2021, the Council adopted a decision on the conclusion of the agreement, the final step in the EU's ratification process.

More specifically, Title III sets out the basis for the EU and the UK to cooperate on digital trade, i.e., trade carried out by 'electronic means'.[49] It is based on a reaffirmation by each party of their respect for the Universal Declaration of Human Rights and other international human rights treaties to which they are parties.[50] And there is an express affirmation of the commitment of each party to high levels of personal data protection, alongside a commitment to work together to promote high international standards and to engage in dialogue, the exchange of expertise, and cooperation on enforcement.[51] The TCA 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 count as a restriction – ranging from data localisation provisions, through to requirements to use locally certified or approved computing facilities.[52]

One element of the TCA that drew criticism was the failure by the Commission to faithfully reproduce in the text of TCA horizontal EU provisions on cross-border data flows and protection of personal data and privacy in the Digital Trade Title of EU trade agreements endorsed by the European Commission in 2018.[53] The relevant clauses in the TCA do not state that data protection is a fundamental right which could lead to arguments that it does not warrant the same level of protection as other fundamental rights, not least because a second clause contains wording that could give rise to conflict if EU laws protecting privacy and related to data protection were challenged in a trade dispute as the EU would need to justify its data protection and privacy laws under strict tests based on Article XIV of the General Agreement on Trade in Services.[61]

Whilst the Commission's actions, in 'watering down' the horizontal clauses were expedient in bringing UK-EU trade negotiations to a conclusion, and are moot now that the UK has secured an adequacy decision and data transfers have been brought under the GDPR framework, the Commission's approach could prove short-sighted should other third countries such as Australia who are engaging in trade negotiations with the EU seek to negotiate the inclusion of similarly broad horizontal provisions in any trade agreement it secures with the EU. Repeated inclusions of such clauses in trade negotiations could have the effect of 'watering down' the EU's high standards of data protection over time, if the third country did not also proceed to seek an EU adequacy assessment. Unsurprisingly, the European Data Protection Supervisor expressed regret and concern that 'In amending the legal wording of the horizontal provisions, the TCA unnecessarily creates legal uncertainty as to the Union's position on the protection of personal data in connection with EU trade agreements and risks creating friction with the EU data protection legal framework.'[54] In an effort to calm the waters¥ and reassert the EU's commitment to high standards of data protection the EDPS has invited the Commission to 'clearly reiterate its commitment to the horizontal provisions as the only basis

[49] Art DIGIT.2, TCA.

[50] Art COMPROV.4, TCA.

[51] COMPROV.19, TCA

[52] The provision is to be reviewed three years; Art 6, TCA.

[53] European Commission, 'Horizontal Provisions on Cross-border Data Flows and Personal Data Protection' (news release of 18 May 2018) http://e c .europa .eu/ newsroom/ just/ item- detail.cf m ?item _id = 627665 accessed 31 May 2021; See also: European Commission, EU proposal for provisions on Cross-border data flows and protection of personal data and privacy, http:// trade .ec .europa .eu/ doclib/ docs/ 2018/ july/trado c _157130 .pdf accessed 31 May 2021. [61] Title X.

[54] EDPS, EDPS Opinion on the conclusion of the EU and UK trade agreement and the EU and UK exchange of classified information agreement, Opinion 3/2021, (22 February 2021), https://edp s .europa .eu/ system/ files/202 1 -02/ 2021 _02 _22 _opinion _eu _uk _tca_e n .pdf, 8.

for future trade agreements by the EU with other third countries, and [to confirm] that personal data protection and privacy rights will not be up for negotiation'.[55]

4.1 TCA Transitional Data Protection Arrangements

The Trade and Cooperation Agreement does not, however, include an adequacy decision to facilitate EEU-UK personal data transfers. 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.[56] The TCA is silent on adequacy because as explained above, an adequacy assessment is a separate process. And although the Commission had agreed to commence its assessment of UK adequacy, using the powers conferred to it by Article 45(3) of the GDPR, in parallel with the trade negotiations, the assessment was not complete by the time the negotiations ended.

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. It provided that the UK would not be treated as a third country for GDPR purposes for a 'specified period' that began on 1 January 2021 and would end either on the date on which an adequacy decision in relation to the UK was adopted by the European Commission under Article 45(3) of the GDPR, or after four months (i.e., until 1 May2021), a period which could be extended by two months by agreement, i.e., until 1 July 2021, if extra time were needed to complete the assessment.[57]

However, the transition period was conditional on the UK not amending its data protection legislation or exercising 'designated powers' such as recognising other third countries as adequate for data transfer purposes, or approving new codes of conduct, certification mechanisms, binding corporate rules, standard contractual clauses or administrative arrangements during the 'specified period,' since changes could jeopardise a finding of adequacy.[58] The only permitted changes were those made to ensure alignment with rules applicable in the EU, for example recognising the new Standard Contractual Clauses (SCC), when adopted by the EU.[59] If the UK otherwise changed its data protection laws or exercised any of the designated powers without consent, the bridging mechanism and specified period would automatically end.

---

[55] Ibid., 10–11; See also: Svetlana Yakovleva, Kristina Irion, 'Pitching trade against privacy: reconciling EU governance of personal data flows with external trade' (2020) International Data Privacy Law, 10(3), 201–221.

[56] Declarations referred to in the Council Decision on the signing on behalf of the Union, and on a provisional application of the Trade and Cooperation Agreement and of the Agreement concerning security procedures for exchanging and protecting classified information, 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

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

[58] Art FINPROV.10A (3), TCA.

[59] EU Commission, 'Data Protection -Standard Contractual Clauses for Transferring Personal Data to Non-EU Countries (Implementing Act)' (*Have your say*) https://e c .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 19 April 2021.

5. POST-TRANSITION DATA PROTECTION IN THE UK AND ADEQUACY REGULATIONS

Given the need for close alignment with the GDPR to initially secure an adequacy decision, and to maximise the likelihood of renewal of an adequacy decision in due course, it should come as no surprise that the UK data protection law is in essence a facsimile of the GDPR. 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 (hereafter 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.[60] For instance, references to EU institutions and procedures were removed and replaced with appropriate post-transition terms e.g., references to 'Union or Member State law' were replaced with references to 'domestic law', and references to decisions made by the EU Commission were replaced with references to decisions made by the UK government. The DPA 2018 was similarly revised.[61] The fundamental principles, obligations on data controllers and processors, and rights for individuals remain the same.

As for transfers of personal data outside the UK they are only permissible if an adequacy decision or appropriate safeguard is in place, or, where a derogation applies. To this end, the DPPEC Regulations provide that derogations continue to be available, and all Binding Corporate Rules (BCRs) authorised, and EU Standard Contractual Clauses issued by the EU before the end of the transition period continue to be recognised as valid by the UK, but any new SCCs must be submitted to the ICO or respective EU supervisory authorities. Likewise, a BCR-holder is required to transfer to the appropriate lead authority and appoint a representative, in the relevant jurisdictions.

The UK also ensured that data flows could continue by preserving all EU adequacy decisions adopted by the EU prior to the end of the transition period (e.g., in respect of Andorra, Japan 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 also been recognised as offering an adequate level of protection, no doubt because Gibraltar is a British overseas territory.

These steps offer certainty and continuity of data flows in the short term, but in recognition of the UK's 'reclaimed' regulatory autonomy, power is conferred on the UK Secretary of State for Digital, Culture, Media and Sport (DCMS) to conduct its own adequacy assessments in respect of transfers outside the UK.[62] Little information is available on the criteria the UK intends to use to assess adequacy apart from public statements that it intends to adopt an outcomes-based risk assessment approach in the hope that they will be concluded more

[60] SI 419/2019, Schedule 1

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

[62] Section 17A, DPA 2018; See also the Memorandum of Understanding between the Secretary of State for Digital, Culture, Media & Sport and the UK Information Commissioner's Office with respect to new UK adequacy assessments following the UK's departure from the European Union, signed on 19 March 19, 2021, https://ww w.go v .uk/government /publications /memorandu m- of -understanding-mou- on
-the -role -of -the -ico -in -relation -to -new -uk -adequacy -assessments/ memorandum -of -understanding -mou -on- the- role -of- the- ico -in -relation- to -new -uk -adequacy- assessments accessed 19 April 2021

speedily than adequacy assessments by the EU.[63] What is known is that an adequacy assessment will involve four phases, the first of which is 'gatekeeping', that is, the process by which a specific team within DCMS will consider whether to commence an assessment of a third country (territory or sector therein) or international organisation for adequacy purposes. This phase will be followed by an 'assessment',[64] that is, the programme of work associated with collecting and analysing information relating to the level of data protection in another country, which will be followed by the third phase, namely a recommendation to the secretary of state, and finally a 'procedural phase', during which an *adequacy regulation* (the UK equivalent of an adequacy decision) will be drafted and laid before the Westminster parliament. The ICO and DCMS are expected to meet for discussions at various intervals during the assessment process, and the secretary shall consult the ICO (and other persons they consider to be appropriate) but the secretary of state has ultimate responsible for issuing adequacy regulations and is not bound by the views of the ICO.[65]

The secretary of state will maintain a list of countries, territories, sectors, and organisations deemed adequate. If the secretary of state determines that a country does not provide an adequate level of protection, then data flows could be restricted - through a refusal to make an adequacy regulation or the revocation or of an existing *adequacy regulation* if one exists.[66]

6. AN 'UNSTABLE' ADEQUACY DECISION

As outlined above, the UK's application for an adequacy assessment was not finalised by the time the TCA was concluded. It was continuing as a separate, parallel process. The UK government had to demonstrate to the Commission that the UK provides an adequate i.e., essentially equivalent level of protection to that in the EU by meeting the criteria in Article 45 of the GDPR and elaborated on in the EDPB's 'adequacy referential,'[67] and corresponding CJEU case law. When assessing adequacy, the Commission was not merely concerned with assessing whether the UK had an appropriate legislative framework regarding data protection, it also had to make a normative judgment about the UK's political structures and values, including respect for the rule of law and respect for human rights and fundamental freedoms. This necessitated an assessment inter alia of UK data protection law and derogations therein, an assessment of data protection procedures and practices and oversight and enforcement measures, a review of surveillance powers in the Investigatory Powers Act 2016, and of provisions to facilitate onward transfers of EEA data from the UK to third countries. To this end, the UK government submitted to the Commission a series of policy documents entitled the 'Explanatory Framework for Adequacy Discussions',[68] covering a wide range 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.

---

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

[64] Art 45 UK GDPR.

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

[66] DCMS, Memorandum of Understanding on the role of The ICO in relation to New UK Adequacy Assessments, 19 March 2021, https://ic o .org .uk/ media/abou t- the- ico/mou /2619468 / uk -adequacy -assessments -ico -dcms- memorandum- of- understanding.pdf .

[67] Article 29 Working Party, 'Adequacy Referential' (2018), wp254rev.01.

[68] HMG, Explanatory framework for adequacy discussions, (13 March 2020) https://ww w .gov .uk/ government/publications /explanator y- framework- for -adequacy- discussions accessed 31 May 2021.

Many deficiencies in UK laws and practices that could prove a bar to a finding of adequacy were identified, including an overly broad immigration exemption in the UK's Data Protection Act 2018, the UK government's decision not to retain the EU Charter in UK law and declarations of an intention to 'opt out' of parts of the European Convention on Human Rights, or at least from interpretations of the Convention by the European Court of Human Rights,[69] and concerns that the Investigatory Powers Act 2016 does not contain substantive limits and safeguards powers regarding retention of and access to bulk data for national security purposes to be compatible with EU fundamental rights law,[70] and relatedly that UK membership of the Five Eyes Intelligence Sharing Alliance posed problems in relation to onward transfers of data from EEA countries to the US especially, but also to other third countries without an adequacy decision in place.[71]

Given these deficiencies, the EU 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[72] was met with consternation in some circles, particularly amongst those who had called for the Commission to adopt a pure or strict approach to interpretation of the legal provisions and standards.[73] Those of us who have followed the Commission's work in the field, in particular its track record of adopting of two deficient adequacy decisions in respect of the US, were less surprised that once again the Commission took account not only of data protection considerations but also political and economic considerations when conducting its assessment.[74]

Thereafter the European Data Protection Board (EDPB) was asked to provide its opinion on UK adequacy. It noted '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 on automated decision-making and profiling. It also noted the UK's stated intention to diverge from the GDPR and, on that basis, welcomed

[69] Owen Bowcott, *UK government plans to remove key human rights protections*, *The Guardian*, (13 September 2020), https://ww w .theguardian.com /law /2020 /sep / 13/ uk- government- plans -to - remove- key -human -rights -protections accessed 31 May 2021.

[70] Ian Brown and Douwe Korff, The inadequacy of UK data protection law Part One: General inadequacy, https://ww w .ianbrown .tech/ wp -content/uploads / 2020/ 10/ Korff -and -Brown -UK - adequacy.pdf accessed 19 April 2021, and The inadequacy of UK data protection law in general and in view of UK surveillance laws, Part Two: UK Surveillance, https://ww w .ianbrown .tech/w p - content/uploads /2020 / 11/ Korff -Brown -Submission -to -EU- re -UK -adequacy -Part -Two- DK-IB201130.pdf, accessed 19 April 2021and Case C-623/17, Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, ECLI:EU: C: 2020: 790.

[71] Ibid.; See also: Oliver Patel and Dr Nathan Lea, 'EU-UK Data Flows, Brexit and No-Deal: Adequacy or Disarray? UCL European Institute, August 2019, https://ww w .ucl .ac .uk/ european -institute/ sites/ european- institute/files / eu -uk _data_flow s _brexit_an d _no _deal _updated.pdf , accessed 31 May 2021.

[72] European Commission, Draft Commission Implementing Decision 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://e c .europa .eu/ info/ sites/ info/ files/ draft _decision_o n _the _adequate _protection _of _personal _data _by _the _united _kingdom _ - _general _data _protection _regulation _19 _feb _2020 .pdf accessed 19 April 2021.

[73] Douwe Korff, The inadequacy of the EU Commission's Draft GDPR Adequacy Decision on the UK, (03.03.2021) https://ww w.ianbrow n.tech / 2021/ 03/ 03/ the -inadequacy -of -the -eu -commissions - draft -gdpr- adequacy- decision -on -the -uk/ accessed 31 May 2021.

[74] Karen Mc Cullagh, 'EU-UK Trade Deal: Implications for Personal Data Transfers' Blogdroiteuropeen, (06.01.21) https://blogdroiteuropee n.com / 2021/ 01/ 06/ eu -uk- trade- deal- implications -for -personal -data -transfers -by -karen -mc -cullagh/ accessed 31 May 2021.

the Commission's proposal to limit an adequacy decision to four years and to closely monitor developments in the UK in the interim. As regards surveillance powers and concomitant oversight powers and safeguards, the EDPB opinion welcomed the creation of the UK's Investigatory Powers Tribunal and its ability to review access to data by UK national security agencies, and 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. Nevertheless, the EDPB opinion raised concerns related to national security monitoring, bulk interceptions, independent oversight related to the use of automated processing tools, and the lack of safeguards under UK law related to overseas disclosure of data, especially for national security exemptions, and recommended that the Commission further assess and/or closely monitor these deficiencies.[75]

A few weeks later, MEPs passed a resolution in the European Parliament on the draft adequacy decision in which they asked the Commission to modify its draft decision that the UK data protection provides an adequate level of protection and concomitantly that data can safely be transferred there pending rectification of several deficiencies.[76] Several MEPs made reference to a research paper that identified deficiencies including[77] shortcomings in the implementation of EU data protection standards linked to the immigration exemption, the overly broad definition of personal data in the Digital Economy Act 2017, weak enforcement of data protection rules by the UK Information Commissioner's Office, potential liberal onward transfer of data to the US, the UK's wavering commitment to EU data protection and human rights standards i.e., stated intention to diverge, and UK surveillance laws and practices pertaining to bulk surveillance and data retention practices that do not comply with CJEU and ECtHR law.[78]

Shortly thereafter the Court of Appeal in England and Wales ruled in *R (Open Rights Group and the 3million) v Secretary of State for the Home Department and Others*, that an exemption in the UK Data Protection Act 2018 which disapplied many data subject rights such as the right of subject access or erasure when personal data was processed for 'the maintenance of effective immigration control' or the 'investigation or detection of activities that would undermine the maintenance of effective immigration control' – at least to those matters which would be prejudiced by complying with the data subject rights, was unlawful because it was overly broad and therefore incompatible with Article 23 of the GDPR and, by extension, the UK GDPR.[79]

These criticisms prompted the Commission to make some changes to its draft adequacy decision prior to adoption on 28 June 2021, a mere two days before the expiration of the TCA bridging mechanism facilitating EEA-UK personal data transfers. Significantly, the adequacy

[75] 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, https://edp b .europa .eu/ sites/ edpb/ files/ files/file1 /edp b _opinion142021 _ukadequacy_gdp r .pdf _en .pdf accessed 19 April 2021.

[76] European Parliament, "Press Release: Data protection: MEPs urge the Commission to amend UK adequacy decisions, (21.05.21) https://ww w .europarl .europa .eu/ news/ en/ press -room/

[77] IPR04124/ data -protection -meps -urge -the -commission -to -amend -uk -adequacy -decisions accessed 31 May 2021.

[78] European Parliamentary Research Service, EU-UK private-sector data flows after Brexit: Settling Adequacy, PE 690.536 – April 2021, https://ww w .europarl .europa .eu/ RegData/etudes / IDAN/ 2021/ 690536/ EPRS _IDA(2021)690536 _EN.pdf accessed 19 April 2021.

[79] *The Open Rights Group & Anor, R (on the Application of) v The Secretary of State for the Home Department & Anor* [2021] EWCA Civ 800. The Court deferred a decision as to appropriate relief, pending further submissions from the parties. It may well be that the DPA 2018 will now need to be amended.

decision does not, at present, cover transfers of personal data to the UK for immigration control purposes, in response to the Court of Appeal judgment which ruled that the immigration exemption in the DPA 2018 is unlawful. The Commission has, however, indicated a willingness to reassess this exclusion once it has been remedied under UK law.[80]

As regards surveillance measures, the Commission stated in a press release accompanying the adequacy decision that it was satisfied the UK system provides an adequate level of protection because the collection of data by UK intelligence authorities is limited to what is strictly necessary to achieve the legitimate objective in question, subject to prior authorisation by an independent judicial body, and individuals have the ability to seek redress via the UK Investigatory Powers Tribunal.[81] Nevertheless, criticism has been expressed that the Commission did not properly scrutinise UK law to ensure compliance with EU law, such that it could be the subject of a legal challenge and suffer a similar fate to the Safe Harbor and its successor Privacy Shield, adequacy decisions, that is, revoked.[82]

The adequacy decision may prove unstable for another reason, namely that adequacy decisions are 'living' documents that need to be 'closely monitored and adapted when developments affect the level of protection ensured by the third country'[83] To this end, the adequacy decision provides an automatic review of the UK legal regime within four years, and it will automatically expire on 27 June 2025 if the Commission has not made a renewed finding of adequacy by then.[84] This reflects the Commission's awareness that as a third country the UK could seek to diverge from the GDPR, and its other international obligations. As Věra Jourová, Vice-President of the Commission for Values and Transparency, explained, 'we have listened very carefully to the concerns expressed by the Parliament, the Members States and the European Data Protection Board, in particular on the possibility of future divergence from

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

[81] European 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, C(2021) 4800 final, https:// ec .europa .eu/ info/ files/ decision -adequate -protection- personal -data- united -kingdom -general- data -protection- regulation_en , para 275.

[82] Korff contends inter alia that the decision completely fails to assess (or even note) the UK's intelligence agencies' actual surveillance practices*;* Douwe Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, Executive Summary, (3 March 2021) KORFF-The-Inadequacy-of-the-EU-Commn-Draft-GDPR-Adequacy-Decision-on-the-UK-Executiv e-Summary-210303final accessed 19 April 2021 and Douwe Korff, The inadequacy of the EU Commission Draft GDPR Adequacy Decision on the UK, (3 March 2021) KORFF-The-Inadequacy-o f-the-EU-Commn-Draft-GDPR-Adequacy-Decision-on-the-UK-210303final accessed 19 April 2021; Vincent Manancourt, 'UK data flows get Brussels' blessing, with caveats,' (*Politico*, 17 April 2021), Two campaigners, speaking on the condition of anonymity, told *Politico* that they were looking to raise funds for a potential legal challenge.

[83] European Commission, 'Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World' (Communication No COM (2017) 7 Final, European Commission, 10 January 2017, 8–9.

[84] European 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, C(2021) 4800 final, https://e c .europa .eu/ info/ files/ decision- adequate-protection -personal -data- united -kingdom -general- data -protection- regulation_en , accessed 31 May 2021, para 289.

our standards in the UK's privacy framework'.[85] The Commission is undoubtedly aware of the UK's vacillating and contradictory statements on the European Convention of Human Rights,[86] as in the statement accompanying the draft decision the Commission stated: 'the UK is – and has committed to remain – party to the European Convention of 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'.[87] Clearly, withdrawal from the European Convention of Human Rights and/or the ambit of the associated court, or other changes to the UK's legal framework e.g., regarding surveillance laws, or onward transfers to third countries, or drifting judicial interpretation by UK courts of core concepts such as the definition of personal data, or failure to revise the DPA 2018 in light of ECtHR and CJEU judgments such that the UK no longer provides an adequate level of protection, could prompt early review of the adequacy decision and its revocation or non-renewal.

7. LONGER-TERM: CONTINUED ALIGNMENT V DIVERGENCE

Evidently, Brexit has added to the complexity of the UK, and indeed, global data protection landscape. And, as Celeste astutely observed,

> Brexit does not achieve its long-awaited objective of freeing UK data protection law from the bridles 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.[88]

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',[89] will be welcomed by those seeking evidence of the UK reclaiming its sovereignty and boldly seeking to forge new or stronger trade links with countries beyond the EU, it is important to note that the UK's own adequacy status, (i.e., adequacy decision facilitating EEA-UK personal data transfers), could be imperilled if the UK were to make a finding of adequacy in respect of countries that the EU has not found adequate and allow such adequacy regulations to be used as a 'back door' for onward transfers of data from EEA countries that would breach GDPR requirements.

---

[85] European Commission, Press Release: Data protection: Commission adopts adequacy decisions for the UK, 28 June 2021, https://e c .europa .eu/ commission/presscorner / detail/en / ip _21 _3183 accessed 31 May 2021.

[86] Owen Bowcott, *UK government plans to remove key human rights protections*, *The Guardian*, (13 September 2020), https://ww w .theguardian .com/law /2020 / sep/ 13/ uk -government- plans- to -remove- key -human -rights -protections accessed 31 May 2021.

[87] European Commission, Press Release: Data protection: European Commission launches process on personal data flows to UK, 19 February 2021, https://e c.europ a .eu/ commission/presscorner / detail/en / ip _21_66>1 accessed 31 May 2021.

[88] Edoardo Celeste, 'Cross-border data protection after Brexit'," *DCU Brexit Institute Working Paper Series*, No 4/2021, 12.

[89] ICO and DCMS, Joint Statement: Secretary of State for the Department for Digital, Culture Media and Sport and the Information Commissioner sign Memorandum of Understanding on data adequacy, 19 March 2021 https:// ico .org .uk/ about -the -ico/new s -and -events/ news -and -blogs/ 2021/ 03/ secretary -of -state -for -the -department -for -dcms -and -the -information -commissioner -sign -memorandum -of -understanding/ accessed 19 April 2021.

Likewise, although the UK can, as a sovereign third country, revise the UK GDPR and DPA 2018, significant divergence could jeopardise the EU-UK adequacy decision and/or impede its renewal. The power to diverge is therefore best described as illusory. And, as 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. Not only that, but Brexit has made the data protection landscape more onerous for multinationals operating in both jurisdictions because both the UK GDPR and the GDPR have extra-territorial effect. Consequently, the compliance burden for data controllers and processors that process data in both jurisdictions has increased because of the need to appoint a representative in each jurisdiction. Relatedly, a data breach that has a multi-country dimension may require notification of both the ICO and at least one EU supervisory authority of the breach, and a supervisory authority in both jurisdictions could investigate and impose sanctions e.g., fines. This change has already prompted some US-owned companies such as Facebook and Google to transfer all their UK users into user agreements with the corporate headquarters in California, to avoid potential legal action in both the EU and UK.[90] These restrictions and dependencies have prompted some to question whether the UK should, in the longer term, strive for regulatory divergence.

The PM has indicated such an intention in a written statement: 'The UK will in future develop separate and independent policies in areas such as […] data protection.'[91] Likewise, the UK's Secretary of State for Digital, Culture, Media and Sport Oliver Dowden MP observed that:

> The EU doesn't hold the monopoly on data protection. So, having come a long way in learning how to manage data risks, the UK is going to start making more of the opportunities. Right now, too many businesses and organisations are reluctant to use data – either because they don't understand the rules or are afraid of inadvertently breaking them. That has hampered innovation and the improvement of public services and prevented scientists from making new discoveries. Clearly, not using data has real-life costs.[92]

Comments of this nature have fuelled speculation that the UK will seek to forge its own data protection path. One proposal suggests replacing the UK GDPR with a new 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, focusing instead on 'whether automated profiling meets a legitimate or public interest test', on the basis that it would reduce onerous compliance burdens and improve the UK's ability to innovate using personal data.[93]

---

[90] Joseph Menn, 'Exclusive: Facebook to move UK users to California terms, avoiding EU privacy rule, (*Reuters*, US Legal News, 15 December 2020), https:// www .theguardian.com /technology /2020 / dec/ 15/ facebook -move -uk -users -california- eu -privacy- laws accessed 19 April 2021; Joseph Menn, 'Exclusive: Google users in UK to lose EU data protection – sources, (*Reuters, Technology News*, 19 February 2020), https://ww w .reuters.com /article /u s -google -privacy -eu- exclusive-idUSKBN20D2M3 accessed 19 April 2021.

[91] PM Statement, UK / EU relations: Written statement – HCWS86, 3 February 2020.

[92] Oliver Dowden, 'New approach to data is a great opportunity for the UK post-Brexit' (*Financial Times* 27 February 2021), https://ww w.f t .com/ content/ac1cbae f- d8bf -49b4 -b11d -1fcc96dde0e1 accessed 19 April 2021.

[93] The Taskforce on Innovation, Growth and Regulatory Reform (TIGRR), Independent Report, (16 June 2021), https://asset s .publishing .service.go v .uk/ government/uploads / system/ uploads/ attachment _data/file /994125 / FINAL _TIGRR _REPORT _ _1 _ .pdf accessed 19 April 2021, 49–53.

The UK is not alone in 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)',[94] a concern that was also identified in the UK National Data Strategy.[95] And, Axel Voss, MEP, one of the strongest proponents of the GDPR has asserted that 'the GDPR is not made for blockchain, facial or voice recognition, text and data mining [. . .] artificial intelligence'.[96] He claims 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.[97]

He has also asserted that 'the coronavirus pandemic also highlighted how the GDPR has prevented better health management, as its provisions hampered the use of tracing apps or even the exchange of data between local authorities for contacting potential vaccine recipients'.[98]

In my view, some of these criticisms are unfounded, or at least a indicate misunderstanding of how data can be processed in compliance with the GDPR.[99] As acknowledged by the Commission, SMEs should be offered additional support e.g., templates, hotlines, and appropriate training to help them understand and meet their GDPR obligations.[100] As for the GDPR impeding innovation, it must be noted that the GDPR does contain lots of 'white spaces' including wide exemptions for research which, if properly developed, will support the UK's world-leading research.[101] If the initial 'teething problems' regarding support for SMEs can be overcome, and the ICO develops guidance explaining how UK-based data controllers and processors can and should interpret the derogations and 'white spaces' in the GDPR, then

---

[94] 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 https://eu r -lex .europa .eu/ legal- content/ EN/ TXT/HTML / ?uri = CELEX: DC0264 & from =EN accessed 19 April 2021.

[95] DCMS, Policy Paper, National Data Strategy, 9 December 2020, https:// www .gov .uk/ government/ publications/u k- national- data -strategy/nationa l- data -strategy accessed 19 April 2021.

[96] Javier Espinoza, "EU must overhaul flagship data protection laws, says a 'father' of policy," (*Financial Times*, 3 March 2021).

[97] Axel Voss, 'How to bring GDPR into the digital age,' (*Politico*, 25 March 2021) https://ww w .politico.eu / article/gdp r -reform -digital- innovation/ accessed 19 April 2021.

[98] Ibid.

[99] For instance, the ICO has produced guidance for health and social care organisations explaining how personal data may be processed during the coronavirus pandemic, along with guidance for employers conducting workplace testing and for businesses collecting personal data for contact tracing <https:// ico .org .uk/ global/ data -protection -and -coronavirus -information -hub/ data -protection -and -coronavirus/ > accessed 19 April 2021.

[100] 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), 9.

[101] For example, scholars have already developed a concept of functional anonymisation in order to allow greater use to be made of personal data for research purposes. Elliot, M, O'Hara, K, Raab, C, O'Keefe, C.M., Mackey, E, Dibben, C, Gowans, H, Purdam, K and McCullagh, K., 'Functional anonymisation: Personal data and the data environment*,'* (2018) *Computer Law & Security Review*, 34 (2) 204-221.

multi-national data controllers are unlikely to call for the UK government to significantly diverge from the GDPR if it continues, on the whole, to meet their needs because 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, significant UK divergence from the GDPR would not necessarily be an appropriate response given that customers increasingly value high levels of data protection,[102] and multi-national companies operating in both the EU and UK are likely to promote continued compliance with the GDPR than a multiplicity of different standards.

If the UK were to diverge from the GDPR in the future, such divergence could take several forms. For instance, the UK could follow the US approach in seeking a partial adequacy decision) akin to the US-EU Privacy Shield (e.g., in respect of only the digital and financial sectors of the UK economy), and a different lower standard e.g., Convention 108+ for other personal data processing, given that the UK has ratified this convention already.[103] However, doing so would require at least two parallel standards of privacy and data protection in the UK e.g., a high level, the GDPR-compliant protection for data that is the subject of EU-UK adequacy decision transfers and a separate, lower, (e.g., modernised-Council of Europe Convention 108) level of protection for other data. The UK could alternatively seek to diverge wholly from the GDPR and focus on complying with Convention 108+. If the UK (and other countries were to pursue this course of action the GDPR could lose influence over time.[104] But, in my view calls for divergence from the EU standard are not likely to be loud or pressing for as long as the EU remains an important trading partner of the UK, and multi-nationals operating on a global basis support compliance with the EU standard.

8. CONCLUSIONS

This chapter opened by arguing that UK's departure from the EU would serve as an acid test not only of the EU's influence as a trade power and global regulator in general, but more specifically, whether the GDPR has any realistic prospect of becoming the 'global digital gold, standard of data protection'.

---

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

[103] Technically, Convention 108+ is formed of the original Convention 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108). The Convention is complemented by a supplementary protocol setting out further requirements as regards data protection regulation and transborder personal data flows. See Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS 108)) and an amending instrument, namely, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 223). As per Article 37 of that Protocol it will only generally apply once all Parties to Convention 108 have ratified it or on or after 11 October 2023 so long as there are at least 38 Parties to this amending protocol: Council of Europe, *Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (2018), <https://r m .coe .int/conventio n-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1> accessed 19 April 2021.

[104] 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; Graham Greenleaf, 'Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives,' (2017) UNSW Law Research Paper No. 17-3, 2.

Despite protracted and at times rancorous negotiations the parties did eventually agree the terms of a trade and cooperation agreement and the UK retained the GDPR in domestic law and applied for an EU adequacy decision under the GDPR framework having conceded that its request for bespoke arrangements would not be entertained, so in that respect the GDPR adequacy framework can be considered a success. Not only that, but the extra-territorial provisions and mutual adequacy obligations in both the UK GDPR and GDPR have created the conditions for synergy and continued alignment between the two data protection frameworks, with the benchmark of protection being the high standard set in the GDPR, at least for so long as each want to facilitate 'free flows' of data to the other.

Whilst Brexiteers are likely to be disappointed at this outcome given their vociferous calls to restore complete sovereignty, data protection advocates will extol the UK's continued compliance with the GDPR as early evidence of the influence of the GDPR and its effectiveness in in ensuring high standards of data protection in third countries around the world.

Having said that, continued compliance by the UK with the GDPR should not be taken for granted. Rather, it must remain fit for purpose. Accordingly, the EU should not ignore the concerns raised that it hampers innovation and competitiveness. If such concerns are not addressed, trade and market forces could act as drivers for divergence from EU data protection law in the longer term. If that were to occur then the EU may not realise its goal of the GDPR becoming the 'global digital gold, standard of data protection'.

In sum, EU data protection advocates have rightly framed the UK's continued compliance with the GDPR as early evidence of the potential for the EU to set the standard of data protection laws and encouraging harmonisation on a global basis, but its longer-term future is not so certain as the GDPR could lose influence over time if it is not fit for purpose. Hence, the UK has left the EU but not EU data protection law behind, for now, at least.