Brexit: Potential Implications for Digital and 'Fintech' industries

Dr Karen Mc Cullagh
UEA LAW SCHOOL
k.mccullagh@uea.ac.uk

Contents

INTRODUCTION

Following the outcome of the historic 'Brexit' referendum on 23rd June 2016 in which a majority of eligible voters in the UK voted to 'Leave,'[1] the United Kingdom is potentially on course to leave the European Union,[2] but to ensure continued economic success it will seek to maintain a favourable trading relationship with the EU. This article identifies and critically evaluates the various types of trade deals the UK might negotiate upon exit with a particular focus on trade in services since financial and digital services are key components of the UK economy. Also, as personal data processing underpins these service industries, particular attention will be paid to the data protection implications that would flow from such agreements. Specifically, it will be of assistance to Mr Matt Hancock, MP as it responds to his predecessor, Baroness Neville-Rolfe's, call to

> 'consider carefully what might be done either to replace it [Regulation (EU) 2016/679] if and when it ceases to have effect or, instead, if in the event it never comes into force. … the future might take several different forms and we need to identify as quickly as possible how to best react to whatever path is eventually chosen.'[3]

This report offers both pre and post exit guidance on the data protection permutations of each type of trade deal. This timely analysis will be of use to policy makers, trade negotiators and businesses as they prepare for a trade and data protection legal landscape outside the European Union; one in which personal data will remain a key economic asset that will continue to be collected, processed and transferred across UK and EU borders.

---

[1] Eligible voters in the UK voted to leave the EU by 52% to 48%. Leave won the majority of votes in England and Wales, whereas Remain won the majority of votes in Northern Ireland and Scotland; <http://www.bbc.co.uk/news/politics/eu_referendum/results>

[2] Leading constitutional scholars and legal practitioners share the view that the referendum result is merely 'advisory' that is, the UK government would need to take further steps to formally notify the EU of its 'decision' to invoke Article 50 of the Treaty on European Union, and commence negotiations on a withdrawal agreement from the European Union with the European Council – a process that could take two (or more) further years to finalise.

[3] DCMS, Speech by Baroness Neville-Rolfe DBE CMG, Parliamentary Under-Secretary of State for the Department for Business, Innovation and Skills and Minister for Intellectual Property, 'The EU Data Protection Package: the UK Government's perspective,' at the Privacy Laws & Business Annual Conference on Data Protection (4th July 2016), <https://www.gov.uk/government/speeches/the-eu-data-protection-package-the-uk-governments-perspective>. The paper will be of value to her successor, Mr Matthew Hancock, MP.

THE ECONOMIC VALUE OF PERSONAL DATA

When the UK withdraws from the European Union (EU) it will want to maintain a trading relationship with it as the EU is the world's largest trading bloc and the world's largest trader of manufactured goods and services.[4] In 2015, the UK exported £223 billion of goods and services to other EU member states, compared to £95.1 billion to the US and £15.9 billion to China.[5]

The service industries account for approximately 78% of the UK's Gross Domestic Product (GDP),[6] and within the services sector, financial services are key - accounting for circa 8% of the UK economic output and approximately 3.5% of employment.[7] Indeed, half of the world's largest financial firms have their European headquarters in the UK and more foreign banks operate in the UK than any other country,[8] plus the UK facilitates 74% of the EU's foreign exchange trading and 40% of global trading in euros.[9] Similarly, the Office for National Statistics has reported that 29% of all financial service exports in the G7[10] are from the UK.

The financial services sector is supported by 'Fintech' industries, that is, companies that use technology to disrupt or make financial services more efficient.[11] The Fintech industries are a subsector of digital technology businesses[12] which represent a further 10% of the UK's services sector, the highest percentage of any G20 member;[13] and

---

[4] European Commission, EU position in world trade, 2 October 2014, at http://ec.europa.eu/trade/policy/eu-position-in-world-trade/index_en.htm.

[5] ONS, UK Economic Accounts, Quarter 4 2015, Table B6B.

[6] ONS, Statistical bulletin: Index of Services: Apr 2016.

[7] Bank of England, Speech given by Mark Carney, Governor of the Bank of England, 'The European Union, monetary and financial stability, and the Bank of England,' 21 October 2015.

[8] Ibid.

[9] Confederation of British Industry, 'Our Global Future: The Business Vision for a reformed EU,' (CBI Report, London, 2013) 137.

[10] The G7: Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States are the seven major advanced economies as reported by the International Monetary Fund: their countries represent more than 64% of the net global wealth ($263 trillion). The European Union is also represented within the G7.

[11] Fintech includes both facilitators (those supporting the technology infrastructure within financial institutions) and disruptors (those challenging current systems with new innovative methods) of finance. Examples include: Transferwise: An International money transfer business, and, Funding Circle: A peer-to-peer business lending firm. Ernst & Young, (2014) 'Landscaping UK Fintech: Commissioned by UK Trade & Investment,' at http://www.ey.com/Publication/vwLUAssets/Landscaping_UK_Fintech/$FILE/EY-Landscaping-UK-Fintech.pdf, 3.

[12] Digital technology businesses are defined as business that provides a digital technical service/product/platform/hardware, or heavily relies on it, as its primary revenue source; Tech City UK & NESTA, (2016) 'Tech Nation 2016: Transforming UK Industries,' at http://www.techcityuk.com/wp-content/uploads/2016/02/Tech-Nation-2016_FINAL-ONLINE-1.pdf?utm_content=buffer2e58f&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer, 9.

[13] G20 is an international forum for the governments and central bank governors from 19 individual countries, namely, Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, South Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, the UK, the United States, and the European Union (EU).

employs 1.56million people.[14] The sector had a turnover in 2014 of £161bn and this figure is set to increase as the sector grew 32% faster than the rest of the UK economy in the period 2010-2014 and is continuing to grow.[15]

The potential for further growth of digital technology businesses was acknowledged in the Queen's speech opening parliament a month prior to the Brexit referendum. In it the UK Government announced an intention to introduce legislation to ensure that the UK would become 'a world leader in the digital economy.'[16] In so doing, the UK hoped to play a leading role in achieving the EU's goal of developing a 'digital single market' projected to be worth €415bn euros to the European Union's economy.[17] The intention was to capitalize on existing success as more than a third of European 'unicorns,'[18] that is, privately owned 'start-up' technology firms worth over $1bn (including Asos, Zoopla, and Fintechs such as Transferwis eand Funding Circle[19]) are currently based in the UK.

Both the digital technology businesses and financial services sectors generate and rely upon huge volumes of personal data in their operations (e.g. in the form of customer records, behavioural, profile and transactional data). Such is the economic value of this personal data that it is sometimes referred to as the 'oil of the Internet and the new currency of the digital world.'[20] Indeed, personal data is recognised as a highly valuable 'new asset class,'[21] and the European Commission has confirmed that 'the value of European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020.'[22] Much of this personal data is transferred across national boundaries for processing and storage on servers in data centres - as a result, the UK hosts the largest data centre market in Europe, and the third largest in the world.[23]

---

[14] note 11, 10.

[15] Ibid.

[16] Cabinet Office, Her Majesty's most gracious speech to both Houses of Parliament at the State Opening of Parliament 2016, 18 May 2016 at https://www.gov.uk/government/speeches/queens-speech-2016

[17] European Commission, A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen, (Press Release, 6 May 2015) at http://europa.eu/rapid/press-release_IP-15-4919_en.htm.

[18] GP Bullhound, 'European Unicorns 2016: Survival of the fittest,' (June 2016)http://www.gpbullhound.com/wp-content/uploads/2016/06/GP-Bullhound-Research-European-Unicorns-2016-Survival-of-the-fittest.pdf>, 5, London is home to 18 unicorns – more than double the number of the next closest country, Sweden, which is home to seven.

[19] Asos is an online fashion and beauty store; Zoopla is a residential property market website. Transferwise is an international money transfer business, and Funding Circle is a peer-to-peer business lending firm.

[20] M. Kuneva, European Consumer Commissioner Keynote Speech, Roundtable on Online Data Collection, Targeting and Profiling, (Brussels, 31 March 2009), at http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm, 2.

[21] World Economic Forum, 'Personal Data: The Emergence of a New Asset Class,' (February 2011) http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf, 5.

[22] European Commission, (2016) 'The EU Data Protection Reform and Big Data Factsheet,' http://ec.europa.eu/justice/data-protection/files/data-protection-big-data_factsheet_web_en.pdf, 1.

[23] A. Kishore, 'Should UK data centers fear Brexit?,' 26 April 2016 http://www.datacenterdynamics.com/content-tracks/security-risk/should-uk-data-centers-fear-brexit/96068.fullarticle.

Thus, the UK's ability to develop and sustain economic growth in the digital technology and financial sectors of the economy and allied Fintech industries and data centres will hinge on a number of inter-related factors that are outlined below.

One factor is 'passporting'[24]: at present, once UK-based financial services providers such as a bank or insurance company are capitalised and regulated in the UK in accordance with EU-wide rules they can provide their services in any other EU or EEA[25] country directly or through a branch without setting up a further capitalised and regulated subsidiary. If, upon Brexit, the UK lost passporting rights and access to the internal market (sometimes referred to as the 'single market')[26] then UK financial services providers would have to set up a capitalised subsidiary within an EEA country (as is the case with Swiss financial service providers) in order to provide services directly or through branches in the whole of the EU. If that were to occur then financial service providers might choose to move their place of establishment outside the UK, thereby impacting on the UK's economy.

It would also impact on the allied Fintech industries. For instance, although the UK with a population circa 68m is a good sized market in which to start a Fintech company, growth would require unimpeded access to the EU's internal market of circa 500m. Speculation that UK Fintechs could, as an alternative strategy, seek to 'scale up' in other large economies such as the US or China overlooks the fact that 50 separate state approvals would be required in the US and that it is very difficult for foreign companies to succeed in China without entering local partnerships. Thus, if UK-based Fintech companies were not able to access the EU's internal market they might decide to maintain access to the internal market by relocating to an EU member state, negatively impacting on the UK's economy.

A further factor that would influence the decision on where to locate is free movement of people as the UK suffers from a digital skills shortage; at present over 30% of the UK's Fintech human capital is from the EU and overseas (20.7% are from EU countries and 13.3% from non-EU countries), so any restrictions on movement of people from EU member states to the UK could impact on firms' ability to recruit suitably skilled workers.[27]

An overarching factor that will influence whether the financial services, digital technology and allied Fintech and data centre industries decide to remain in the UK or relocate to other EU member states is the legal and regulatory environment, specifically, the data protection rules that govern the processing and transfer of personal data. It is not clear whether the UK will, in a post-Brexit era, choose to voluntarily align its data protection laws with those of the EU or seek develop its own framework. There has been some speculation that Brexit will provide an opportunity to reduce red-tape concerning data transfers and allow the UK to develop a more business-friendly data

[24] Financial Conduct Authority, 'Passporting,' https://www.the-fca.org.uk/firms/passporting.

[25] The EEA includes EU countries and also Iceland, Liechtenstein and Norway. The EEA Agreement allows EEA countries to participate in the EU's internal market.

[26] The European Union (EU) is an economic and political union of 28 countries. It operates an internal (or single) market which allows free movement of goods, capital, services and people between member states.

[27] Wayra, 'UK more diverse than other major start-up ecosystems, including the US, Silicon Valley, NYC and Tel Aviv,' 14 June 2015, http://wayra.co.uk/uk-more-diverse-than-other-major-start-up-ecosystems-including-the-us-silicon-valley-nyc-and-tel-aviv/.

protection environment as the largely self-regulatory approach in the online world is often cited as an element in the success of US digital technology companies.
However, if the UK leaves the EEA and does not implement data protection laws that closely mirror the provisions in the forthcoming Regulation (EU) 2016/679, *Visa* may have to relocate its data centre operations (with a loss of hundreds of jobs) from the UK to an EU country as 'an agreement in the recent £17.5 billion takeover of *Visa*'s European operations by its American sister company included a stipulation that data from *Visa* card transactions should not leave Europe.'[28] Other US owned banks such as JP Morgan Chase, Goldman Sachs, Citigroup, Bank of America and Morgan Stanley that historically established their EU operations in the UK due to the ease of sharing a common language, and use it as a base to 'passport' their services to other countries as well as process and store personal data 'are preparing to shift at least some of their workers to other EU countries'[29] for similar reasons.
Moreover, if financial services, Fintechs and digital sector industries decided to relocate their business from the UK to other EU member states then less personal data would be transferred in and out of the UK for processing and storage purposes, thereby impacting on the UK's data centre sector.
Accordingly, the discussion below provides an overview of data protection in the UK and the EU before exploring three aspects of five (Norwegian, Swiss, Canadian, Turkish and World Trade Organisation) trade deal models to illustrate the advantages and disadvantages of each for the digital technology and Fintech sectors of the UK economy. Firstly, access to the internal market in goods, capital, services (with a particular focus on digital and Fintech services) and people (i.e. a focus on the ability to recruit IT specialists). Secondly, requirements to follow EU rules and regulations (specifically 'financial passporting' and data protection) and, thirdly, ability to exert influence over future EU laws and regulations (especially the financial services sector of the internal market and data protection). Given that personal data processing underpins the financial, digital technology and Fintech industries, the data protection implications of each trade deal are also considered.

DEVELOPMENT OF EU DATA PROTECTION LAWS

The UK first introduced data protection legislation in 1984 in response to pressure from the business community, which voiced concerns that the UK would lose cross border trade in personal data if it remained a 'data haven.' For instance, in 1974, the Swedish Data Inspection Board blocked the export of personal data to the UK for the preparation of embossed health identity cards. The Swedish authority cited the terms of its 1973 Data Act and the UK's lack of legal protection as justification for the restrictions.[30] The impetus at the international law level for the government to introduce data protection legislation in the UK came with the publication of two international legal instruments

[28] M. Kleinman, 'Brexit Jobs Threat At Credit Card Giant Visa,' *Sky News*, 1 July 2016, http://news.sky.com/story/brexit-jobs-threat-at-credit-card-giant-visa-10327664.

[29] M. Arnold, & L. Noonan, 'Banks begin moving some operations out of Britain,' *The Financial Times*, 26 June 2016.

[30] Written assurances by the UK contractor that no copies of the tapes would be made and that their security conditions were stringent were not considered adequate; M. Adams, 'Sweden prohibits sending data to UK,' *New Scientist*, 17 April 1975, 133.

on data protection in the early 1980s: the OECD Guidelines in 1980[31] (which reaffirmed privacy as a fundamental human right and stated that cross-border personal transfers should be subject to adequate safeguards) and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981[32] which guaranteed the protection of personal data as a separate right granted to an individual. It also provided for the free movement of personal data between countries that had ratified the Convention with restrictions potentially being placed on the movement of data outside that group. Only countries whose domestic law provided equivalent safeguards to those defined in the Convention could ratify. Thus, when the Convention was opened for signature in January 1981, the UK government was motivated to sign and implement it by economic considerations - a failure to do so could have given other countries reason to divert personal data flows away from the UK thereby undermining the competitiveness of British industry.

Whilst the UK and other countries did enact national data protection laws, it became apparent in the late 1980 s that national regulators could not ensure compliance with national legislation once personal data had left their jurisdiction. For instance, in 1989, the French data privacy authority (CNIL) blocked the transfer of personal data about employees and customers from Fiat France to the parent company, Fiat Italy, arguing that the absence of data protection laws in Italy rendered the transfer illegal.[33] As a temporary solution Fiat was required to sign a contract with CNIL that it would guarantee privacy protection for any information transferred from France.[34] The political and economic impact of such personal data transfer disputes led to calls for a supra-national data protection law to facilitate and manage cross-border data flows. On 11 September 1990, the European Commission responded by a proposing a directive on the processing of personal data,[35] which, after five years of intense politicking and lobbying, came to fruition in the form of Directive 95/46/EC (hereafter ' the Directive').[36] Each Member state has implemented the Directive's provisions through the domestic implementing laws. In the UK, the Directive was implemented through the Data Protection Act 1998 (DPA 1998).[37]

---

[31] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; On 11 July 2013 the OECD Council adopted a revised Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data ('Privacy Guidelines'), Part 4, Para 17 states: A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.

[32] The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No 108.

[33] J. Fauvet, 'Privacy in the New Europe,' *Transnational Data & Communications Report*, (Nov 17-18, 1989) cited in A. Meunier & K.R. McNamara (eds) *Making history: European Integration and Institutional change at fifty* (OUP, 2007).

[34] *Transnational Data and Communications Report*, 'No fiat for Fiat,' 10 November 1989.

[35] C 277 Official Journal of the EU, 5 Nov 1990, 3.

[36] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281/31.

[37] It repealed the Data Protection Act 1984. The DPA 1998 applies to England & Wales, Scotland, N. Ireland, and is overseen by the ICO.

The Directive seeks to advance the establishment and functioning of an internal market in personal data through harmonization of member states' data protection laws. It seeks to do so through the promotion of two objectives, namely, i) that member states should protect an individual's right to privacy with respect to the processing of personal data through the approximation of member states' (and EEA states) laws on the protection of personal data whilst, ii) also facilitating the free flow of personal data among the member states and EEA countries.[38]

The Directive also recognises that the free flow of personal data to and from 'third' countries beyond the EU and EEA such as the USA, Canada, and Switzerland is necessary for international trade. To ensure that privacy concerns about transfers of personal data to such countries do not cripple international trade, Article 4 provides a wide scope of territorial application of the Directive whilst Article 25 requires that third countries ensure 'adequate' protection of the personal data. Article 4(1)(a) applies to the processing of personal data if such processing 'is carried out in the context of the activities of an establishment of the controller' in the EU. The CJEU interpreted the notion of the processing of personal data 'in the context of activities of an establishment' very broadly in two recent cases. In *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*[39] the CJEU held that a data controller owned by an entity located outside the EU may be subject to the Directive if it has a subsidiary in the relevant Member state's territory which carries out activities which are inextricably linked. Thereafter, in *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság,*[40] the CJEU confirmed that the formalistic approach whereby organisations are considered to be established solely in the place in which they are registered is not the correct approach; rather, the concept of establishment must be interpreted broadly so that it applies to a foreign registered company which exercises, through stable arrangements, real and effective (albeit minimal) activity in that member state.

Furthermore, Article 25(1) only permits the transfer of personal data to a third country with an 'adequate' level of protection on the basis that this will ensure that the high level of that protection continues where personal data is transferred to a third country.[41] To this end, a third country can seek an adequacy determination finding from the European Commission. This involves an abstract assessment by the European Commission of a third country's legal and administrative system in relation to the protection of personal data in light of the particular circumstances of each transfer or set of transfers.[42] If satisfied, the European Commission issues a legally binding 'adequacy decision' confirming the adequate level of protection in the third country, so that transfers of personal data to this third country are lawful.[43] If the European Commission finds that the level of protection in a third country is inadequate, 'EU Member states shall take the measures necessary to prevent any transfer of the same

[38] Art 1 (1) and (2).

[39] Case C-131/12, ECLI:EU:C:2014:317.

[40] Case 230/14, ECLI:EU:C:2015:639.

[41] Ibid, para 72.

[42] Article 25(4) and (6).

[43] Article 25(4) and (6).

kind of personal data to this third country.'[44] To date, the Commission has issued adequacy decisions in respect of eleven countries.[45]

Also, a special sectoral regime to accommodate commercial transfers of personal data between the EU and the US (the Safe Harbour agreement) was formally adopted in an adequacy decision by the European Commission in 2000.[46] However, in *Maximillian Schrems v Data Protection Commissioner*,[47] the CJEU ruled the adequacy decision invalid on the basis that it did not take account of overriding US legislation that permitted US authorities (such as the National Security Agency) to have access to the personal data of EU citizens. The CJEU also ruled that data protection authorities in the EU are not (and should not be) fettered by the Commission's decision on the adequacy of US Safe Harbor (or the data protection laws of other third countries) to provide protection when personal data is transferred outside of the EU. Rather they can and should be free to investigate the adequacy rulings of third countries in response to complaints. This prompted the US and EU to negotiate a new scheme (the Privacy Shield)[48] for transatlantic personal data transfers, which was approved by the EU member states representatives,[49] clearing the way for the adoption of an adequacy decision by the European Commission on 12th July 2016.[50] The Privacy Shield agreement includes principles such as security, accountability for onward transfer, notice, choice, data integrity, purpose limitation, access, recourse, enforcement and liability. Under the new framework, companies transferring personal data between the EU and US must commit to stricter data privacy obligations and publish them. These privacy commitments will be overseen by the US Department of Commerce and enforced by the US Federal Trade Commission. Furthermore, companies processing EU human resources data will be bound by the decisions of the European Data Protection Authorities.[51]

Whilst adequacy decisions and bilateral agreements such as the privacy shield serve a useful function they are also complex and time consuming to negotiate and administer. Thus, Article 26 sets out a number of conditions, which permit the transfer of personal data to a third country that does not ensure an adequate level of protection. First, personal data can be transferred to a third country under one of the conditions set out

---

[44] Article 25(4).

[45] Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay.

[46] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L 215/7.

[47] *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14 [2015] ECLI:EU:C:2015:650, paras 98, 104-106.

[48] U.S. Department of Commerce, EU-U.S. Privacy Shield, at https://www.privacyshield.gov/Program-Overview

[49] Article 31 Committee.

[50] European Commission, Commission Implementing Decision Of 12.7.2016 Pursuant To Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the protection provided by the EU-U.S. Privacy Shield, Brussels, 12.7.2016, C(2016) 4176 final.

[51] European Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield, at http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

in Article 26(1), which includes: the unambiguous consent of the data subject (though the Art 29WP has warned that the consent of the data subject 'is unlikely to provide an adequate long-term framework for data controllers in cases of repeated or even structural transfers for the processing in question')[52] or the performance or conclusion of a contract with or in the interest of the data subject. Secondly, the supervisory authorities of EU Member states can authorise a transfer or a set of transfers of personal data subject to adequate safeguards[53] in the form of binding corporate rules (BCRs), which can be used for international transfers of personal data within a multinational company with establishments in third countries, [54] or through model/standard contractual clauses,[55] that is, pre-formulated contracts which are pre-approved by the European Commission and ad hoc measures such as appropriate contractual clauses.[56]

However, although each member state transposed the Directive's provisions into national laws, they did not do so uniformly,[57] and this led to fragmented application and enforcement. For instance, some countries added clauses to require breach notification; others did not. Similarly, sanctions have varied widely - Spain has fined often and heavily whereas France has rarely imposed fines.[58] Some member states such as the UK and Ireland transposed provisions in a pragmatic, business-friendly way with the effect that many US owned corporates chose to set up a European hub or data centre for processing data from all their European offices in either the UK or Ireland, as a means of avoiding having to deal with EU data transfer restrictions. The lack of harmonization threatened the EU's internal market goals, so the European Commission instigated infringement proceedings against the UK government for failure to properly implement 11 articles in the Directive into the Data Protection Act 1998 (DPA 1998),[59] and this was a key factor in the decision to propose replacing the Directive with a

---

[52] Article 29 Working Party, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (25 November 2005) WP 114, 11.

[53] Article 26(2).

[54] BCRs are modeled on corporate codes of conduct. They are approved by EU Member states' supervisory authorities. Guidance on the approval process can be found in A29WP, 'Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules' (14 April 2005) WP108, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp108_en.pdf

[55] Article 26(4).

[56] Article 26(2) Working Party on the Protection of Individuals with regard to the Processing of Personal Data, 'Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (24 July 1998), 3.

[57] D. Korff, (2002), 'EC Study on Implementation of Data Protection Directive 95/46/EC,' http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE>

[58] C. Tankard, 'What the GDPR means for businesses,' *Network Security Newsletter*, June 2016, at http://digpath.co.uk/wp-content/uploads/NESE_2016-06_Jun.pdf, 5.

[59] C. Pounder, 'European Commission explains why UK's Data Protection Act is deficient,' at http://amberhawk.typepad.com/amberhawk/2011/02/european-commission-explains-why-uks-data-protection-act-is-deficient.html; C. Pounder, 'Copy correspondence between Dr Chris Pounder and EU Commission & Ombudsman,' at http://amberhawk.typepad.com/files/dp_infraction_reasons.pdf>; C. Pounder, 'European Commission raises infraction threat to UK on failing to implement Directive 95/46/EC properly via the Data Protection Act,' athttp://amberhawk.typepad.com/amberhawk/2014/10/european-commission-raises-infraction-threat-to-uk-on-failing-to-implement-directive-9546ec-properly.html; The infraction proceedings are ongoing.

Regulation (as well as a concern that it was no longer fit for purpose due to changes in personal data processing technologies).

PRE-WITHDRAWAL DATA PROTECTION: REGULATION (EU) 2016/679

The European Union member states recently finalized the text of Regulation (EU) 2016/679 that will repeal and replace Directive 95/46/EC. It retains but strengthens some the core principles of Directive 95/46/EC. For instance, the bar for valid consent has been raised much higher. It must be fully unbundled from other terms and conditions and will not be valid unless freely given, specific, informed, and unambiguous, and it must be as easy to withdraw consent as it is to give.[60] Regulation (EU) 2016/679 also introduces several new data subject rights and obligations on data processors and controllers (e.g. right to be forgotten[61] and data portability[62]), and higher sanctions for non-compliance. Significantly, it has a wide extra-territorial application – it will apply not only to controllers and processors of data established in the EU that process personal data but also to organisations established outside the EU, if they process personal data relating to the offering of goods or services to individuals in the EU, or if they monitor the behaviour of individuals in the EU/EEA countries, for example, through cookies.[63] Additionally, it requires non-EU data controllers to designate a representative in the EU.[64] The representative must be established in an EU member state where relevant data subjects are located and act as a point of contact on behalf of the non-EU controller in respect of all issues relating to compliance with Regulation (EU) 2016/679.

[60] Articles 4(11) and 6(1) (a).

[61] Art 17.

[62] Art18.

[63] Article 3 (2).

[64] A representative is not required if data processing: (1) is occasional, (ii) does not extend to the processing of special categories of data (such as biometric data, criminal convictions and/or details of an individual's race, ethnicity, political or religious opinions or sexual orientation) on a large scale, and (iii) is unlikely to result in risk to the rights and freedoms of natural persons taking into account the nature, context, scope and purpose of the processing.

It also includes the introduction of an accountability requirement for data controllers,[65] an increased level of fines,[66] and a 'one stop shop' approach to regulatory oversight,[67] that is, organisations will be regulated by the data protection regulator in the place of their main establishment (i.e. the main administrative location in the EU unless the main decisions about data processing are taken in a different Member state in which case that will be the main establishment). Individuals will be able to make complaints in their member state at which point that regulator will engage in a cooperation procedure which will be settled by the newly established European Data Protection Board in the event of disagreement. Member state regulators will also be able to deal with any issues arising in their own States subject to a cooperation procedure.

As an EU Regulation, it would be directly applicable in the UK without the need for implementing domestic UK legislation as of 25th May 2018. Although Regulation (EU) 2016/679 will repeal and replace Directive 95/46/EC, it will not repeal the Data Protection Act 1998 as domestic legislation can only be amended or repealed by the UK Government. Since it is highly likely that the UK will not have completed the 'exit process' by 25th May 2018, the UK Government will initially be obligated to amend the DPA 1998 to bring UK law in line with the requirements in Regulation (EU) 2016/679.[68] UK based businesses will therefore need to continue to prepare for and be in a position to comply with provisions in Regulation (EU) 2016/679, even if continued membership is expected to be short-lived.

UK DATA PROTECTION POST BREXIT

The situation will change if or when the UK leaves the EU. Withdrawal from the EU will afford the UK an opportunity to pause and reflect on the potential data protection implications of the UK seeking a trading relationship in which they would either be obliged to implement Regulation (EU) 2016/679, choose to do so voluntarily, or opt to devise and implement their own data protection law. Given that some of the provisions in Regulation (EU) 2016/679 were hugely contested by the UK - for instance, Mr Ken

[65] Article 24 requires that organisations implement 'appropriate technical and organisational measures' to be able to 'demonstrate' their compliance with the Regulation, which shall also include 'the implementation of appropriate data protection policies'. Therefore, in preparing for the Regulation, organisations will have to implement not only internal and publicly-facing policies, records and notices, but also technical measures, and fundamental personnel and strategic changes to their processing operations.

[66] A two-tiered sanctions regime will apply. Art 83 (5) & (6). Breaches of some provisions by businesses, which law makers have deemed to be most important for data protection, could lead to fines of up to €20 million or 4% of global annual turnover for the preceding financial year, whichever is the greater, being levied by data watchdogs. For other breaches, Art 83 (4) states that the authorities could impose fines on companies of up to €10m or 2% of global annual turnover, whichever is greater.

[67] Art 77 will allow individuals to make complaints about the misuse of their data with the Data Protection Authority (DPA) in their home country, rather than where the company is based.

[68] Consolidated Version of The Treaty on The Functioning of The European Union (TFEU), Part Six, Institutional And Financial Provisions, Official Journal of the European Union, C 326/1, Article 288; Until the UK completes the process of withdrawal from the European Union, it remains subject to all of its EU obligations, including the obligation to transpose EU Regulations (such as Regulation (EU) 2016/679) into UK law.

Clarke MP, objected to the right to be forgotten,[69] and several MEP's actively lobbied for amendments requested by digital technology companies such as Amazon, and Google,[70] some have suggested that pressure will be brought to bear on the Government for the UK to introduce a data protection framework that less burdensome for small businesses,[71] and is more business-friendly in general.[72] One might think that the introduction of less stringent data protection rules would make the UK more attractive as a trading partner. However, that would not necessarily be the case for two reasons. Firstly, the EU data protection framework (both Directive 95/46/EC and the forthcoming Regulation (EU) 2016/679) are regarded as "gold standard".[73] Indeed, 'over half the countries in the world now have a data protection and/or privacy law, and most are strongly influenced by the European approach.'[74] Complying with a separate, different, UK data protection framework would present an unwelcome additional compliance burden for businesses operating on a transnational basis. Secondly, the adequacy and extra-territorial reach elements of Regulation (EU) 2016/679 will apply to UK based businesses that process the personal data of EU citizens.

Given that UK-based businesses processing personal data of EU citizens will continue to be obliged to comply with Regulation (EU) 2016/679, having to comply with a separate UK data protection framework would represent an additional legal compliance burden – one that would add to the cost of doing business in the UK and put UK businesses at an economic disadvantage. Accordingly, the critical analysis of the implications of the different trade models for financial and digital services below will also consider the data protection implications of each trade model.

POST-EXIT TRADE MODELS & DATA PROTECTION IMPLICATIONS

The UK is the first member state to seek to withdraw from the European Union since its creation. Three former territories of European member states withdrew (Algeria, Greenland and Saint Barthélémy**)**. Whilst not directly comparable, the experience of Greenland is instructive in that it withdrew but sought to maintain a trading

---

[69] Ministry of Justice, Lord Chancellor and Secretary of State for Justice, Rt. Hon Kenneth Clarke MP, Speech at the British Chamber of Commerce in Brussels, 'Data protection,' 26 May 2011, at https://www.gov.uk/government/news/kenneth-clarke-warns-on-eu-data-protection-rules

[70] LobbyPlag at http://lobbyplag.eu/map

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

[72] D. Castro, 'Brexit Allows UK to Unshackle Itself from EU's Cumbersome Data Protection Rules,' 20 July 2016, at http://globaldatinginsights.com/2016/07/20/brexit-allows-uk-to-unshackle-itself-from-eus-cumbersome-data-protection-rules/

[73] G. Buttarelli, 'The EU GDPR as a clarion call for a new global digital gold standard,' (2016) 6 *International Data Privacy Law*, 77-78

[74] G. Greenleaf, 'Global Data Privacy Laws Countries, with European Laws Now a Minority,' (2015) *Privacy Laws & Business International Report,* 109, 133.

relationship.[75] This small country has a population of approximately 56,000 and its economy is dominated by a single industry, fishing (90%). Even so, the withdrawal and renegotiation was lengthy and complex:

> "unpicking EU membership was a long and laborious process. It took three years or so, even when there was just one industry involved, and one product whose access to the European market had to be negotiated…The other major downside is that leaving the control of Brussels did not free them from what the 'Leave' campaign call the dead-hand of Brussels regulation. Far from it. They are no longer at the table when fisheries are discussed, but if they are to sell into the single-market - which they must - then every rule applies to them as much as it does to us."[76]

At present, it is not clear what type of post-withdrawal trading relationship the UK might seek to have with the EU, as the government explicitly ruled out contingency planning;[77] and the 'Leave' campaign did not outline a clear plan,[78] rather it indicated dissatisfaction with the current UK-EU relationship on the basis that the UK could not fully control immigration: *'we need to take back control of our borders so we can decide who comes here – and who can't,'*[79] and had ceded sovereignty to the EU on some aspects of law making and lost the ability to independently negotiate trade relationships with other countries: '*We should negotiate a new UK-EU deal based on free trade and friendly cooperation. We end the supremacy of EU law…We regain our seats on international institutions like the World Trade Organisation so we are a more influential force for free trade and international cooperation.*'[80]
Possibilities include exiting the EU but becoming a member of the EFTA and EEA thereby retaining access to the internal market (the Norwegian model), exiting the EU and joining the EFTA but not the EEA, with limited access to the internal market and relations governed by a framework of bilateral agreements (the Swiss model), or total exit from the EU and the internal market. This latter option could see the UK seek to negotiate free trade agreements with individual countries (the Canadian model), or join the Customs Union (the Turkish model), or access the EU market under the World Trade Organisation (WTO) rules. The analysis of each trade model is accompanied by discussion of the different data protection implications that would flow from each, with particular attention paid to transfers of personal data both within the EU/EEA and to third countries.

---

[75] It remains subject to the EU treaties through association of Overseas Countries and Territories with the EU. This was permitted by the Greenland Treaty - a special treaty signed in 1984 to allow its withdrawal.

[76] J. Mates, 'What lessons can the UK learn from Greenland leaving the EU?,' *ITV News*, 10 May 2016 at http://www.itv.com/news/2016-05-10/what-lessons-can-the-uk-learn-from-greenland-leaving-the-eu/

[77] G. Parker, 'Tories Shun Brexit Contingency Plans', *Financial Times*, 1 December 2015.

[78] See the Leave Campaign website for further information http://www.voteleavetakecontrol.org

[79] Ibid.

[80] Ibid.

The 'Norwegian' EFTA & EEA model

The UK could leave the European Union but join the European Free Trade Association (EFTA) whose current members, Iceland, Liechtenstein and Norway, trade with the EU via the European Economic Area (EEA).[81] This model has a few economic advantages that might, at first glance, appear attractive to those tasked with establishing a new trade relationship who are not in favour of 'ever closer union.' For instance, EEA membership does not oblige countries to participate in monetary union, the EU's common foreign and security policy, common agricultural policy, or justice and home affairs policies. Also, whilst there is free trade within the EEA, members are not part of the EU's customs union, which means that they can set their own external tariff and conduct their own trade negotiations with countries outside the EU. Notably, there is a financial cost associated with being a member of the EEA and internal market - members have to make a substantial contribution to the EU's regional development funds and contribute to the costs of the EU programmes in which they participate, such as co-operation on science and research activities.[82] For instance, in 2011, Norway's contribution to the EU budget was £106 per capita, only 17% lower than the UK's net contribution of £128 per capita.[83]

There are parallels between the UK and Liechtenstein economies in that both are mixed economies, with large financial and service sectors. An EFTA trade deal would be good for UK financial and allied Fintech services because financial regulation would stay largely the same and passporting rights in the EU internal market would be maintained. This would allow UK based Fintechs to continue to 'scale up' their operations across Europe using e-money licenses and passporting arrangements. Also, the UK would continue to participate in EU programmes and strategies, including the 'Digital Single Market Strategy,'[84] which would be of benefit to the UK's growing digital technology sector.

However, to join the EEA, the UK would have to commit to complying with the four freedoms laid down in the Treaty on the Functioning of the European Union (i.e. the free movement of goods, services, people and capital) as these are incorporated in the EEA agreement.[85] The UK could seek to partially disapply provisions in the EEA Agreement regarding the continued free movement of people, using Art 112, that is: 'serious economic, societal or environmental difficulties of a sectorial or regional nature liable to persist are arising,' [86] as Liechtenstein did when it first joined the EEA.

---

[81] The European Economic Area (EEA) was established by several Agreements signed in 1992. It allows the three EEA States to largely participate to the EU's internal market. Admitting the UK as a new State to the EEA would require an accession treaty, which would have to be concluded, not only by the EU and the UK but also by each of the thirty EEA Member states (twenty seven from the EU and three from EEA).

[82] Art 116 EEA Agreement.

[83] House of Commons, (2013), 'Leaving the EU,' Research Paper 13/42, 1 July 2013.

[84] See note 16.

[85] OJ 2012/C 326/01; The EEA was established in 1994 to give European countries that are not part of the EU a way to become members of the internal market.

[86] Art 112 EEA, is intended to be an 'emergency safeguard provision for highly specific obligations;' Prof Dougan offered the view that it would be inappropriate to use Art 112 as a measure to exempt the UK from free-movement requirements. He viewed Liechtenstein as a special case and stated that the UK does not meet the same criteria. House of Commons, Treasury Committee, The UK's future

The UK could seek to further mirror Liechtenstein's experience in introducing a quota system to control the number of people allowed to enter the country to restrict intra-EU migration yet be able to draw upon the IT talent of EU citizens to address the UK's IT skills shortage. However, although Liechtenstein has been permitted to introduce a quota system controlling the number of people allowed to enter the country due to it being 'a very small inhabitable area of rural character with an unusually high percentage of non-national residents and employees,' [87] it is by no means certain that the EU would countenance a restriction on intra-EU migration to the UK as part of any agreement as the countries are vastly different: Liechtenstein is 61 sq mi in size with a population of 37,340 compared to UK 93,628 sq mi, with a population of 65,102,385. Moreover, a unilateral decision by the UK to limit the free movement of persons under the EEA agreement would be subject to review by the EEA Joint Committee[88] who could rule on the 'scope and duration' of the safeguard. The UK would be advised that Art 112 is intended to be an 'emergency measure' and that the EEA agreement permits the EU to implement 'proportionate rebalancing' measures [89] such as restricting 'passported' financial services exports by the UK to the EU (the scope of such measures would also be subject to review by the EEA Joint Committee), so any attempt to limit movement of people could result in an economic cost, as well as political and social controversy.

In the longer term, this model may not be appropriate for the UK because EEA countries such as Norway have to implement EU rules concerning the internal market, including legislation regarding employment, consumer protection, environmental law, financial services and competition policy, but have no influence in the legislative drafting process as they do not have voting power or formal access to the decision-making process since rules of the internal market are set by the EU not the EEA.[90] In particular, the UK would have to submit to the rule that the EEA States 'speak with one voice' in the Joint Committee; in effect one EEA State has the ability to block the transposition into EEA law of a new or revised EU law even if the other EEA States would urgently need that transposition for economic reasons.[91]

Overall, whilst this trade model does not offer all the benefits associated with being a member of the European Union, it is perhaps the next best alternative trade model for the digital economy and financial services sectors of the UK economy. Thus, the potential data protection implications of such a trade deal are considered below.

---

economic relationship with the European Union, 5th July 2016, at http://parliamentlive.tv/event/index/cb083c53-3998-4f3a-8eca-e114e3dbdf0b (11.45mins onwards).

[87] Liechtenstein issues residence permits for 56 workers and 16 non-workers each year, half of which are decide by a lottery held twice each year. This arrangement was given formal status by an amendment to Annex VIII of the EEA Agreement, setting out what were called "sectoral adaptations," cross-referred to Annex V on the free movement of workers. The measures are subject to review every five years.

[88] Art 113 EEA.

[89] Art 114 EEA.

[90] Agreement on The European Economic Area, *OJ No L 1, 3.1.1994,* Article 102, at http://www.efta.int/media/documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEAagreement.pdf

[91] Article 93 EEA Agreement.

Data protection implications of the 'Norway' model

Data protection within the internal market has been harmonized and is part of the EEA agreement.[92] Accordingly, Regulation (EU) 2016/679 would be directly applicable in the UK as an EEA country. In the short-to-medium term, this model would be advantageous, as it would provide legal certainty for UK established businesses. UK established data controllers and processors would continue to be obligated to ensure fair and lawful processing of personal data. From a digital technology and Fintech perspective this model is advantageous as transfers of personal data from EU and EEA countries would continue without restrictions. It would avoid the problems outlined above, wherein *Visa* stipulated that the personal details of its European customers must be stored in data centres in Europe, in response to concerns about privacy and data protection in third countries.

Under Regulation (EU) 2016/679, transfers of personal data from the UK to non-EEA countries would be prohibited in the absence of an adequacy determination by the European Commission.[93] Model clauses would continue to provide an alternative mechanism for transfers from the UK to non-EEA countries that have not obtained an adequacy finding from the Commission, subject that is, to the outcome of a preliminary reference to the CJEU on the legal status of data transfers under such clauses.[94] Similarly, UK data controllers could continue to use Binding Corporate Rules (BCRs) for data transfers to non-EEA countries. These would continue to be reviewed and authorized by the ICO (UK data protection regulator). Furthermore, UK based data controllers and processors would be permitted to use the 'Privacy Shield' for transfers to the US. The Regulation (EU) 2016/679 'one-stop-shop' would apply, that is, responsibility for the supervision of processing of data controllers or data processors whose 'main establishment' is in the UK (they may have a presence in other Member states) would be allocated to the ICO. Also, should the UK opt to join the EEA, individuals and UK courts would be obliged to refer data protection matters to the EFTA Court. Under the EEA Agreement rules, the EFTA Court 'pays due account to the principles laid down by the European Court of Justice's case law',[95] so the UK

---

[92] EEA, Article 36, Annex XI, data protection laws are to be implemented into the internal legal order of EEA states. A special adaptation text was adopted at the time of incorporation of the Data Protection Directive, stating that Commission decisions pursuant to Article 31 of the Directive, concerning e.g. transfer of data to third countries should apply temporarily as regards the EFTA EEA states without regard to pending incorporation of those Acts into the Agreement, provided that the EFTA EEA states would not decide otherwise and inform the Commission accordingly; See, Joint Committee Decision No 83/1999 (OJ No L 296, 23.11.2000, p. 41 and EEA Supplement No. 43, 23.11.2000, p. 112 (I) and p. 81 Del 2 (N)), e.i.f. 1.7.2000.

[93] Under Article 45 of Regulation 2016/679, the European Commission may assess whether a country has an adequate level of data protection by taking into account: the rule of law, respect for human rights and fundamental freedoms, and other legislative enactments and case law, he existence and effectiveness of an independent supervisory authority with adequate enforcement powers, and International commitments the country has entered into.

[94] An Coimisinéir Cosanta Sionraí, 'Statement by the Office of the Data Protection Commissioner in respect of application for Declaratory Relief in the Irish High Court and Referral to the CJEU,' 25 May 2016,at https://www.dataprotection.ie/docs/25-05-2016-Statement-by-this-Office-in-respect-of-application-for-Declaratory-Relief-in-the-Irish-High-Court-and-Referral-to-the-CJEU/1570.htm

[95] To avoid a race to the bottom and forum shopping, the drafters of the EEA Agreement formulated homogeneity rules that essentially bind the EFTA Court to follow relevant CJEU case law. C. Baudenbacher, 'The EFTA Court and Court of Justice of the European Union: Coming in Parts But Winning Together,' pp. 183-203 in A. Rosas (ed), *The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case-law - La Cour de Justice et la Construction de*

would, in effect, continue to be influenced by rulings made by the EU courts on Regulation (EU) 2016/679. The Fintech and digital economy startups that have established European bases in the UK would welcome these measures.

In the longer term this trade model has, however, several data protection disadvantages relating to a loss of regulatory influence. Firstly, as outlined above, EEA countries such as Norway and Liechtenstein are 'rule takers rather than rule makers,' that is, they have to implement EU rules concerning the internal market, including financial services and data protection but have no influence in the legislative drafting process as they do not have voting power or formal access to the decision-making process since rules of the internal market are set by the EU not the EEA.[96] Thus, the UK Government would lose legislative influence as it would not have a say or voting rights in respect of any future amendments to Regulation (EU) 2016/679, which could be significant given that the UK has tended to favour a pragmatic, business friendly approach to data protection more so than some of its EU member state counterparts. Relatedly, the ICO could become a less influential body as it would not have participation rights in respect of membership of the forthcoming European Data Protection Board (a reconfigured Article 29 Working Party[97]), an EU body with legal personality and extensive powers to determine disputes between national supervisory authorities, to give advice and guidance and to approve EU-wide codes and certification.[98]

In summary, the UK would benefit from passporting and access to the internal market but would lose the right to influence the laws on the internal market (including data protection) or the bodies responsible for their implementation.

The 'Swiss' EFTA & bilateral treaties model

The UK could seek to replicate the arrangement Switzerland has in place in that it could negotiate to leave the European Union and join the European Free Trade Association (EFTA) (but not the EEA), which provides for free trade with the EU in all non-agricultural goods, and negotiate bilateral treaties to govern other trade relations with the EU. For example, Switzerland has entered into bilateral treaties with the EU on insurance, air traffic, pensions, and fraud prevention, to name a few.[99] The combined effect of EFTA membership and bilateral agreements covering technical barriers to trade is a similar level of goods market integration with the EU for Switzerland as EEA countries. The perceived advantage of the bilateral treaty approach is that it would allow the UK the flexibility to choose EU initiatives in which it wished to participate,

---

l'Europe: Analyses et Perspectives de Soixante Ans de Jurisprudence, (T.M.C. Asser Press, 2013).

[96] Agreement on The European Economic Area, *OJ No L 1, 3.1.1994,* Article 102, at http://www.efta.int/media/documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEAagreement.pdf

[97] The Article 29 Working Party, whose members were the EU's national supervisory authorities, the European Data Protection Supervisor ("EDPS") and the European Commission has been transformed into the "European Data Protection Board ("EDPB"), with similar membership but an independent Secretariat.

[98] Regulation (EU) 2016/679, Recitals 139 & 140, and Chapter VII Section 3.

[99] Approximately 120 bilateral agreements currently exist between the EU and Switzerland; European Commission, Trade, Countries, Switzerland, at http://ec.europa.eu/trade/policy/countries-and-regions/countries/switzerland/index_en.htm

and freedom to remain uninvolved in those that are not of economic, social or political interest. Another positive aspect of this model is that Switzerland has made lower contributions to the EU in respect of regional funding and the costs of the programmes in which it participates: approximately £53 per capita, which is 60% lower than the UK's net contribution per capita.[100] Lower funding contributions would be attractive to the UK.

Nevertheless, there are legal, social, and political costs to this model. For instance, Switzerland has almost no influence over the design of the EU programmes in which it participates. Additionally, the treaties negotiated with the EU require Switzerland to implement policies and legislation set by the EU. At present, there is also free movement of people between Switzerland and the EU, although in February 2014, Switzerland voted in a referendum to impose restrictions on immigration from the EU that would violate its agreement with the EU on free movement of people. It remains to be seen whether or how the Swiss government will implement this vote and what will be the consequences for Swiss-EU relations. If future Swiss–EU trade relations become contingent on free movement of people, the Swiss bilateral trade model will be a less attractive option for UK negotiators who want freedom of movement for IT workers to address the UK's digital skills shortage yet otherwise restrict immigration to the UK.

The factor that is, however, most likely to persuade UK trade negotiators that this is not the most appropriate model for the UK is that Switzerland and the EU have not reached a comprehensive agreement covering trade in services. Consequently, Switzerland is not part of the internal market for services and Swiss financial institutions wanting to serve the EU market have to do so through subsidiaries based in EU Member states (predominantly London, at present). If the UK were unable to secure a bilateral agreement on trade in services it could, in theory, allow the UK regulator (Financial Conduct Authority) to make its own decisions about what regulation is best for UK financial firms and result in a reduced regulatory burden for UK Fintechs since EU rules would no longer apply. However, it is more likely that, if the UK lost its passport, this would encourage US and other foreign owned banks currently based in the UK to move trading operations to Paris and Frankfurt and back-office data centre operations to Dublin. Thus, a loss of passporting rights would negatively impact on the financial and digital services sectors and allied Fintech and data centre industries. In effect, it could drive Fintech investment and data centres from the UK into other European countries, with a related loss of jobs and negative impact on the UK economy.

A trade deal of this type may not even be on the negotiating table as a possible option as it was originally designed to be a unique transitional measure pending the full membership of Switzerland in the EU and the EU has expressed concerns about its long-term viability (it has commenced negotiations, which if implemented, would go further than the provisions of the EEA, i.e. being more demanding for Switzerland than for the EEA Members).[101] The EU may not entertain any similar relationship with the UK, particularly if it is unwilling to accommodate free movement of people.

---

[100] House of Commons, (2013), 'Leaving the EU,' Research Paper 13/42, 1 July 2013.

[101] In May 2014, the EU commenced negotiations with Switzerland on "*an international agreement on an institutional framework governing bilateral relations with the Swiss confederation*" which, if agreed would require future agreements to include provisions giving a role of surveillance to the European Commission, as well as a possible judicial control to the EU Court of Justice. The agreement would also impose on Switzerland a maximum time-limit for the implementation in Swiss law of changes to the *acquis communautaire* decided unilaterally by the EU.

Even so, the potential data protection implications of the Swiss trade model are considered below as they illustrate how and why the UK might voluntarily choose to closely mirror the provisions of Regulation (EU) 2016/679 in any post-withdrawal data protection legislation.

Data Protection Implications of the Swiss model

The EU data protection framework governing EU and EEA countries does not extend to EFTA only countries, so Switzerland, as a 'third' country was not obligated but rather chose voluntarily to mirror the provisions Directive 95/46/EC in its legislation (The Swiss Federal Data Protection Act 1992). It further sought and received an "adequacy" decision from the European Commission,[102] allowing it to freely transfer and receive personal data from its nearest and most economically important trading partners - EU member states. It also uses model clauses and binding contract rules to transfer data to non-EEA countries. Of note is that although Switzerland is not subject to the jurisdiction of the Court of Justice of the European Union (CJEU), its case law has had a significant influence on Swiss legislation. For instance, after the CJEU invalidated the European Commission's Decision on the EU-U.S. Safe Harbor arrangement,[103] the Swiss Federal Data Protection and Information Commissioner (FDPIC) declared that the Swiss-US Safe Harbor agreement (which mirrored the EU-US Safe Harbor agreement but also covered personal data of legal entities) did not provide a sufficient legal basis for exporting data from Switzerland to the U.S.[104]

The degree of influence of EU data protection law on Switzerland will increase as of 25th May 2018, when Regulation (EU) 2016/679 will not only be applicable for Swiss companies based in the EU (or their subsidiaries in the EU), but also for Swiss based companies that are offering goods or services to EU data subjects as the extra-territorial scope of Regulation (EU) 2016/679 will also include organizations processing personal data of EU data subjects, or organisations that monitor the (online) behaviour of EU data subjects.[105] Therefore, numerous Swiss organizations that currently have no local presence in the EU will be within the territorial scope of the Regulation. If, going forward, Switzerland does not revise the Swiss Federal Data Protection Act 1992 to reflect changes in Regulation (EU) 2016/679 then the European Commission could

---

[102] 2000/518/EC Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C (2000) 2304), Official Journal of the European Communities L 215/1, 5/08/2000 P. 0001 - 0003

[103] The Safe Harbor Agreement was negotiated between the US Department of Commerce and the European Commission to enable businesses to transfer EU data to the US in compliance with the EU Directive 95/46/EC (now being replaced by Regulation (EU 2016/679). Only organizations that self-certified against Safe Harbor privacy principles were legally permitted to transfer EU data to the US. In Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, An Austrian Facebook user lodged a complaint with the Irish DPA after the Snowden revelations had shown that his data and that of other EU citizens had been accessed by US intelligence services. The Safe Harbor Agreement was invalidated.

[104] Federal Data Protection and Information Commissioner (FDPIC), Further information on the transfer of data to the USA, 28 June 2016, athttp://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01325/index.html?lang=en

[105] Article 3 (2).

revoke its adequacy decision, after determining that as a third country, Switzerland no longer has comprehensive data protection laws of an equivalent standard. To avoid this, the Swiss Federal Council outlined that 'it is economically important for Switzerland to be recognized as a country with an appropriate data protection level for the EU,' and engaged the Federal Department of Justice and Police to draft a revised Data Protection Act which gives 'due consideration of the EU data protection regulation.' The revised Act is scheduled to come into effect around the same time as Regulation 2016/679.[106]

If the UK chose to withdraw from the EU, join the EFTA and negotiate bilateral agreements with the EU as Switzerland has, then it might also seek to replicate the Swiss legal arrangements regarding personal data transfers to the EU, EEA and other countries. In the unlikely event that the UK withdraws from the EU prior to 25th May 2018, that is, whilst Directive 95/46/EC is still in force, it could choose to follow the Swiss model in seeking an adequacy decision from the European Commission. One might expect the UK to easily obtain an 'adequacy' decision given that it has implemented Directive 95/46/EC into domestic law in the form of the DPA 1998.

However, the DPA 1998 will almost certainly not be adequate, because as outlined above, the UK was (and remains) the subject of infringement proceedings for deficient implementation of key provisions of Directive 95/46/EC, the effect of which were a more pragmatic and business-friendly approach to data protection than most other EU Member states.[107]

Equally, if the UK withdraws from the EU after the 25th May 2018, it should ensure that any revisions to the DPA 1998 closely mirror provisions in Regulation (EU) 2016/679, otherwise an adequacy determination may not be forthcoming from the Commission. A positive adequacy determination cannot, however, be predicted with certainty at this stage given the UK's (and Information Commissioner's Office's) persistent pushback on large tracts of the draft Regulation that they considered either overly process-driven or unnecessarily protective of the individual, as such views could influence any post-withdrawal amendments made to the DPA 1998.

In making an adequacy decision the European Commission would also be influenced by the CJEU decision in *Maximillian Schrems v Data Protection Commissioner*, which questioned the adequacy of the protection afforded to EU data subjects' personal data when transferred to the US,[108] as well as the forthcoming preliminary reference in respect of the Joined cases *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis*.[109] These factors would also impact on any negotiations to devise a UK-US privacy shield. Whilst there could be support in both the US and UK for a Regulation-lite framework in relation to data flows regarding UK and US citizens, the UK will likely be required

[106] Swiss Federal Department of Justice and Police, Federal Council Press Release: 'Data Protection Should be Strengthened,' 1 April 2015, at http://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2015/2015-04-010.html

[107] See note 57.

[108] See note 101.

[109] CJEU, Cases C-203/15 and C-698/15 (forthcoming); The Data Retention and Investigatory Powers Act (DRIPA) 2014 requires internet and phone companies to keep their communications data for a year and regulates how police and intelligence agencies gain access to it, thereby facilitating the mass surveillance of personal data. A judgment is expected later this year.

to demonstrate that the personal data flows it receives from EU member states will not be transferred on to the US under less stringent terms.

Pending an adequacy decision by the Commission (under either Directive 95/46/EC or Regulation (EU) 2016/679), UK based companies operating in the EU, or indeed an EU-based company would need to revise the methods they use to transfer data to the UK (such as Model Clauses or Binding Corporate Rules). This could increase the regulatory burden and costs of UK established businesses that process personal data of EU citizens since these approved mechanisms for lawfully transferring data add an additional administrative layer and vary between jurisdictions. For example, some Member states, such as Spain, require organisations to obtain prior authorisation from the local supervisory authority before making any such transfer.

Moreover, as a 'third country,' some provisions in Regulation (EU) 2016/679 such as the One-Stop-Shop, the European Data Protection Board and Binding Corporate Rules, will not be applicable in the UK (nor will they be in Switzerland). For instance, although UK data controllers could continue to rely on Binding Corporate Rules for data transfers to third countries, the ICO would not formally be part of the Regulation (EU) 2016/679 review procedure nor able to grant authorisations (it remains to be seen whether an informal mutual recognition procedure is agreed, as is the case now). Also, as the one-stop-shop provisions will apply only to EU and EEA based data protection regulators, a UK based data controller subject to both UK (or Swiss) data protection law and Regulation (EU) 2016/679 could face separate enforcement action from both the ICO and other EU DPAs (it is anticipated that there will be a degree of co-operation and information-sharing). Data controllers such as financial service providers, Fintechs and data centres may take the view that their compliance burden would be less onerous if they were based in an EU country rather than having to ensure compliance with two regulators; mass relocations of businesses would inevitably impact upon the UK economy.

In the longer term, the UK might not find this model satisfactory as, being a 'third' country, it would also lose its ability to influence and shape any further revisions of Regulation (EU) 2016/679 and related legislation in the future, which could be significant, given that the UK is viewed as acting as a pragmatic, business friendly counterweight to countries that tend to take a more human rights focused approach to data protection laws.

The 'Canadian' Free trade agreement model

Alternatively, the UK could seek to follow Canada in negotiating a trade agreement with the EU.[110] For example, Canada and the EU have finalized the Comprehensive Economic and Trade Agreement (CETA).[111] When ratified by each member state, (the Canadian government's requirement of a visa for all travellers from Romania and

[110] The Canadian Trade Service Commissioner, 'Exporting to the EU - A Guide for Canadian Business,' at http://tradecommissioner.gc.ca/european-union-europeenne/market-facts-faits-sur-le-marche/0000256.aspx?lang=eng

[111] European Commission, Comprehensive Economic and Trade Agreement (CETA), at http://ec.europa.eu/trade/policy/in-focus/ceta/

Bulgaria has delayed ratification),[112] all of Canada's manufactured exports and 98% of its agricultural goods will be available for sale within the EU internal market without any import tariffs. Canada will not have to make contributions to the EU budget - as Norway does - nor sign up to the free movement of workers - as both Norway and Switzerland are required to do. This aspect of the Canadian free trade model would be attractive for UK trade negotiators as it would allow them to restrict immigration to the UK, yet have freedom to permit immigration of highly skilled IT workers to fill the UK's digital skills gap.

Significantly, CETA is the first third-country agreement in which the EU has agreed to internal market access in the services sector on the basis of a negative list, meaning that all service markets are liberalised except those explicitly excluded. On the face of it, this could provide a promising basis for negotiations between the UK and the EU on freedom to provide services. It does, however, fall short of providing Canadian companies with unrestricted access to EU services markets, which is the entitlement currently enjoyed by UK companies as a result of our EU membership. Specifically, this trade model does not include passporting – Canadian firms seeking to take advantage of the EU financial services 'passport' will have to establish a presence in the EU and comply with EU regulations. [113]

Therefore, if adopted by the UK, the 'Canadian model' would make it more difficult for UK-based financial services firms to trade in the EU internal market, as they would have to set up subsidiaries in the EU in order to operate. It is likely they would move at least some of their operations outside the UK. Consequently, industries allied to the financial services and digital technology sectors of the economy such as Fintechs and data centres would be likely to relocate from the UK to other EU member states, impacting negatively on the UK's economy.

Even if it were possible to negotiate such a trade deal it could not be done quickly or easily – it took seven years to finalise the Canadian agreement (not yet in force). Such a lengthy gap might prove unattractive for UK negotiators as protracted trade negotiations could impact negatively on the UK economy resulting in lost investment and jobs. Moreover, Canada found that it had little influence in the negotiation phase regarding the terms of the agreement, nor does it have recourse to an independent arbiter if problems arise. Given that the UK will be under pressure to negotiate quickly, they may find it difficult to 'hold out' for preferable terms in a free trade agreement with the European Union.

This approach would be disadvantageous for another reason - the UK would have to negotiate separate trade agreements with non-EU countries as any UK-EU free trade agreement would not include rights and agreements concluded by the EU in relation to third countries (a mammoth task given that the EU has concluded more than two hundred Free Trade Agreements with third States or organisations, covering 35% of world trade). The UK would be at a disadvantage, as it would have much less bargaining power than the EU. Furthermore, a CETA-type relationship with the EU

[112] The Canadian government's requirement of a visa for all travellers from Romania and Bulgaria has delayed ratification. The UK Brexit vote may cause further delay; European Commission, 'Press Release: EU visa reciprocity mechanism – Questions and Answers,' 12 April 2016, at http://europa.eu/rapid/press-release_MEMO-16-1346_en.htm

[113] V. Scarpetta, 'What could the EU-Canada free trade deal tell us about Brexit?,' 15 March 2016, at http://openeurope.org.uk/today/blog/what-could-the-eu-canada-free-trade-deal-tell-us-about-brexit/

would result in the UK being removed from the EU's decision making institutions, so its capacity to influence EU law making would be diminished – instead of exerting influence through participation in the EU's legislative processes it would instead have to impact via diplomacy with the European Commission. Nevertheless, the data protection implications of such a trade relationship are discussed below.

Data Protection Implications of the Canadian model

If the UK implemented the Canadian trade model it could also choose to follow the example set by Canada regarding data protection – The Personal Information Protection and Electronic Documents Act (PIPEDA) was drafted with Directive 95/46/EC in mind, that is, to provide an adequate level of protection for the purpose of data transfers from the EU to Canada. Thus, the UK could revise the Data Protection Act 1998 so that it mirrors provisions in Regulation (EU) 2016/679 and seek an adequacy determination from the European Commission.

However, provisions in domestic law - the Data Retention and Investigatory Powers Act 2014 (DRIPA), which is currently the subject of a preliminary reference to the CJEU in Joined Cases *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis*[114] may preclude an adequacy finding by the European Commission, in which case the UK would either have to amend its law, or, alternatively, UK businesses would have to make use of model clauses and binding corporate rules, both of which are administratively time-consuming and complex to effect.[115]

Theoretically, the UK could adopt a different (lower) standard of data protection for internal UK and non-EU established business. However, although data protection rules are perceived to be burdensome, particularly for small businesses, it is likely that the UK business community would exert pressure on the UK government to implement data protection laws in the UK that provide an equivalent level of protection since Art 3 (2) of Regulation (EU) 2016/679 will apply to the processing of personal data by controllers and processors established outside the EU[116] if their processing is related to offering goods or services, including those provided free of charge, to EU individuals or to the monitoring of individuals' behaviour within the EU/EEA countries.[117] Businesses would not want to see a return to the pre-DPA 1998 days in which data transfers to the UK could be blocked due to privacy and data protection concerns (e.g. the Swedish health ID cards, French-Italy Fiat transfers). Additionally, businesses that are keen to stress their privacy and data protection credentials to boost consumer confidence may find it a 'hard sell,' particularly as the principles in Directive 95/46/EC and the forthcoming Regulation (EU) 2016/679 are regarded as 'as a gold standard or 'spearhead' reference model for personal data protection'[118] both in Europe and

---

[114] See note 107.

[115] A29WP, 'Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995' (25 November 2005) WP 114, 11.

[116] Article 3(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

[117] Article 3(2).

[118] Rand Europe, 'Review of the European Data Protection Directive,' at https://ico.org.uk/media/about-the-ico/documents/1042349/review-of-eu-dp-directive.pdf; K. Irion, S.

beyond, with many other countries replicating this model e.g. the eleven 'adequate' countries, and most recently, Bermuda have been influenced by it.[119] Thus, digital technology, Fintech and data centre businesses that operate on a global basis would question the wisdom of having to comply with multiple laws since it would merely increase their compliance burden.

The 'Turkish' Customs Union model

The UK could seek to follow Turkey's example in entering into a customs union[120] with the EU that allows for tariff-free access without quotas to the internal market for goods but not public procurement or agriculture (the latter is subject to separate bilateral trade concessions negotiated between Turkey and certain EU member states). The advantages of this model are that the UK (like Turkey) would not have to make contributions to the EU budget nor facilitate intra-EU migration.

However, like Turkey, the UK would be required to adopt a common tariff with the rest of the EU for third-country goods and would be restricted in its ability to conclude agreements with other countries without the EU's consent. Moreover, under such an arrangement, the UK would have to accept large sections of the EU's *acquis communautaire* and it is highly likely that the EU would require the UK (as it currently does Turkey) to harmonise its laws with those of the EU in relation to competition, data protection, intellectual property, and consumer protection. If the UK resisted this, the EU might suspend market access or impose anti-dumping duties, to prevent British firms undercutting EU competitors through subsidies or deregulatory measures. Additionally, the UK (like Turkey) would not have any ability to influence the composition of those laws, plus the UK (like Turkey) would have to comply with the decisions of the CJEU where relevant to these areas, whilst not having a Judge as a member of the Court of Justice or as a member of the General Court.

Problematically, this trade model does not cover trade in services so if adopted by the UK, the financial and allied Fintech services sectors would suffer as the UK would lose both its passporting rights and right to provide services on equal terms with EU members unless the UK negotiated access to the EU internal market for services. Even if those hurdles could be overcome, this trade model would not be suitable for the UK in the longer term as, like Turkey, it would not be involved in any future Free Trade Agreements that the EU might negotiate with other countries and would not benefit from them. It would be obliged to negotiate its own, separate trade agreements. For instance, the UK recently established a 'Fintech Bridge' that 'will help UK Fintech

---

Yakovleva and M. Bartl, 'Trade and Privacy: Complicated Bedfellows? How to achieve data protection-proof free trade agreements,' Independent study commissioned by BEUC et al. (Institute for Information Law (IViR), Amsterdam, 2016).

[119] Bermuda is in the process of introducing the Personal Information Protection Act 2016 (Bill), which takes into account the EU General Data Protection Regulation and the EU-US Privacy Shield, as it intends to seek an adequacy finding from the European Commission to allow it to lawfully engage in data transfers of EU citizen's data, at http://www.parliament.bm/uploadedFiles/Content/House_Business/Bills/Personal%20Information%20Protection%20Bill%202016%20AS%20TABLED%20INTHE%20HOUSE.pdf

[120] Decision No 1/95 Of The EC-Turkey Association Council of 22 December 1995 on implementing the final phase of the Customs Union (96/142/EC), at http://www.avrupa.info.tr/fileadmin/Content/Downloads/PDF/Custom_Union_des_ENG.pdf

firms and investors access the Asian market and expand to the Republic of Korea, as well as attracting Korean Fintech companies and investors to the UK.' [121] Whilst this is a welcome development, the UK government will have to negotiate separate agreements for UK Fintechs to access other markets, which would be a time-consuming and complex process – and in the meantime, financial service providers and Fintechs may take the view that it would be simpler and more cost effective for them to relocate from the UK to European member states.

Finally, it is far from certain that the EU would be interested in entering such a trade deal with the UK as the arrangements put in place for Turkey are intended as a transitional precursor to full EU membership, and given that this model would provide only limited access to the EU's internal market, yet would deprive the UK of sovereignty on trade policy, it is difficult to see how it could be attractive to the UK. Nevertheless, the potential data protection implications of the Turkish trade model are considered below.

Data Protection Implications of the Turkish model

In a step toward accession to the European Union, Turkey enacted its first comprehensive data protection law in 2016: Law No. 6668 on the Protection of Personal data[122] which is based largely on the EU Data Protection Directive (95/46/EC) and key aspects of the forthcoming Regulation (EU) 2016/679 e.g. the national data protection authority will have the power impose fines and prison sentences in certain circumstances. In the unlikely event that the UK seeks to implement a customs union trade model it will find that the easiest way to ensure continued personal transfers between the EU and UK will involve revising the Data Protection Act 1998 to ensure compliance with provisions in Regulation (EU) 2016/679 and negotiate a bilateral agreement for the free movement of data to enable the transfer of data between EU/EEA countries and the UK (subject to the comments above regarding DRIPA).

The World Trade Organization model

Currently, the UK is a member of the World Trade Organization (WTO) but, as with all the EU member states, the EU has exclusive competence over common commercial policy.[123] If the UK left the EU without putting in place any of the alternative trade arrangements discussed above, then trade with both the EU and almost all the rest of the world would be governed by the WTO General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS).[124]

---

[121] Financial Conduct Authority, Co-operation Agreement between Financial Conduct Authority (FCA) and Financial Services Commission of the Republic of Korea (FSC), 22 July 2016, at https://www.fca.org.uk/static/fca/documents/mou/fca-korean%20fsc-co-operation-agreement.pdf

[122] The law was passed by the Turkish Parliament 24 March and published in the Official Gazette 7 April 2016.

[123] Art. 3 TFEU.

[124] The WTO has made far less progress than the EU in liberalising trade in services (negotiations between 23 members of the WTO (including the EU) on The Trade in Services Agreement (TiSA) are ongoing); European Commission, Trade in Services Agreement (TiSA), athttp://ec.europa.eu/trade/policy/in-focus/tisa/

Being outside the internal market would enable the UK government to set economic policy and regulatory standards without taking account of the preferences of other EU members but any divergence in regulation between the UK and the EU would still act as a non-tariff barrier to trade and raise the cost of doing business with Europe. As for trade with third countries - it would be governed by the WTO rules, which specify that each member must grant the same 'most favoured nation' (MFN) treatment, that is, accord the most favourable tariff and regulatory treatment given to the product of any one Member at the time of import or export of "like products" to all other Members. The only exceptions to this principle are that countries can choose to enter into free trade agreements such as the EFTA or EU and can give preferential market access to developing countries. As a WTO member, the UK's exports to the EU and other WTO members would be subject to the importing countries' MFN tariffs. Ottaviano et al have calculated that this would raise the cost of exporting to the EU for UK firms compared with EU membership.[125]

Under GATS, WTO members make various reciprocal commitments concerning market access and equal treatment for foreign institutions. However, there is no uniform EU external trade policy for services as the EU's GATS schedule sets out a framework for market access but individual countries have derogations in particular subsectors and modes of supply, so relying upon GATS would not provide UK financial services access to the EU Market on a comparable basis to EU membership.

In the absence of the EU financial 'passport' system, the UK could create its own rules for the regulation of banks, but in practice, these would have to be applied on a non-discriminatory basis and EU banks would thus have to be treated on the same basis as other foreign institutions. Likewise, UK banks operating within the EU would become subject to local supervision - the result - a less favourable outcome for the UK's financial institutions than the EU passporting rules. For financial services and Fintech currently based in the UK, this is the least favourable trade model, as, like the Canadian and Turkish trade models, it does not include passporting in the EU internal market. New Fintechs wishing to serve the wider European market would be less likely to establish themselves in the UK, and other financial service providers would likely relocate at least part of their operations to EU member states to avail of passporting rights.

Even if political appetite existed for this option it would be an incredibly complex process and one that would not necessarily result in economic gains for the UK in all instances as once outside the EU the UK would need to negotiate new agreements with approximately 60 non-EU countries or organisations (together, these FTAs cover about 35 per cent of world trade)[126] and the UK acting alone would have much less bargaining power than the EU as a collective bloc.

It would also be a very time-consuming process – for instance, in relation to a possible WTO trade deal with China: "One estimate currently doing the rounds is that it will take 500 British officials and 10 years to negotiate a fresh trade deal with China,"[127]

---

[125] G. Ottaviano, J. P. Pessoa, T. Sampson, and J. Van Reenen, 'The Costs and Benefits of Leaving the EU', (Centre for Economic Performance Policy Analysis, 2014) at http://cep.lse.ac.uk/pubs/download/pa016.pdf

[126] J. C. Piris, 'If the UK votes to leave: The seven alternatives to EU membership, (Centre for European Reform, 2016), at https://www.cer.org.uk/sites/default/files/pb_piris_brexit_12jan16.pdf

[127] S. Leavenworth, 'Britons showed 'losing mindset', say Chinese media in swipe at leave vote,' *The Guardian*, 25 June 2016.

Plus, the UK doesn't have any expert trade negotiators - as they are all working in the European Commission. As outlined above, this could impact severely upon the financial and digital services sector of the UK economy, making this an unattractive option. Even so, the data protection implications of this model are considered below.

Data Protection Implications of the WTO model

Given the length of time it would take to negotiate trade deals under the WTO trade model, it is highly likely that Regulation (EU) 2016/679 will be in force in the UK, at least in the short-to-medium term. However, if the UK followed the WTO trade model, it would be free to revise its data protection laws, and some have speculated that the UK might welcome the opportunity to set its own data protection standards, ones that are more pragmatic, business friendly and involve less regulatory oversight:

> Liberal laws on data protection could encourage investment in areas such as artificial intelligence, an area that has a tricky relationship with privacy at the best of times and in which Britain excels, as shown by the many acquisitions of home-grown AI businesses by the likes of Google.[128]

In theory, reintroduction of its own legislation (the UK could opt to retain a similar model to that currently in place under the DPA 1998) would enable the UK to reduce restrictions on personal data flows out of the UK to the rest of the world. Developing trade links with other countries such as Japan, Malaysia, Russia and Singapore would, however, be dependent upon the UK continuing to offer 'adequate' levels of protection for cross-border personal data transfers of at least the level in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981. As for UK-EU personal data transfers, whilst the UK would not (in theory) have to comply with CJEU jurisprudence, Art 3 (2) of Regulation (EU) 2016/679 would apply to the processing of personal data by controllers and processors established outside the EU (including the UK) if their processing is related to offering goods or services, including those provided free of charge, to EU individuals or to the monitoring of individuals' behaviour within the EU/EEA countries.[129] Consequently, not aligning UK data protection laws with provisions in Regulation (EU) 2016/679 (and any related CJEU jurisprudence) could create compliance difficulties for UK established organisations seeking to engage with EU citizens because the UK would be obliged to seek an 'adequacy' finding from the European Commission. This might be further complicated by provisions in the Data Retention and Investigatory Powers Act 2014 (DRIPA) that are currently the subject of a preliminary reference to the CJEU in Joined Cases *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis*.[130] If an adequacy finding was not forthcoming, it would likely prejudice the UK from receiving business from EU member states as UK established businesses would have to put arrangements in place in order to send personal data to the UK as a 'third country' such as reliance upon unambiguous consent, model clauses or binding corporate rules to effect data transfers.

---

[128] J. Titcomb, 'We mustn't let Brexit open a chasm with Europe on data protection,' *The Telegraph,* 30 June 2016.

[129] Article 3(2).

[130] See note 107.

In addition, the UK would also lose the advantage of the limited "one-stop shop" concept introduced by Regulation (EU) 2016/679 meaning compliance with two sets of laws and consequently, exposure to two sets of sanctions for non-compliance. In these circumstances, it is likely that some organisations might choose to move their business headquarters out of the UK and arrange for another EU location to become their "main establishment" and another Data Protection Authority to become their lead authority. Thus, any potential competitive advantages for UK businesses might be quickly negated by the compliance costs associated with the regulatory burden of compliance with different data protection regimes. For these reasons, it is highly likely that the UK government would not introduce amendments to UK data protection law that would cause significant deviations from Regulation (EU) 2016/679.

CONCLUSIONS

The foregoing analysis illustrated that leaving the European Union will negatively impact the financial services and digital economy sectors of the UK economy. Given the importance of these sectors to the UK's future economic prosperity, steps should be taken to mitigate the impact of Brexit. The discussion confirmed that whilst the Norwegian model would be the best alternative trade model (because it would allow the UK to retain passporting rights and access to the internal market) and that the WTO trade model would be the least favourable trade model for financial and Fintech services, none of the trade models discussed are wholly suitable for the UK. Thus it is highly likely that the UK will seek to negotiate a unique, hybrid deal that 'cherry picks' elements from existing trade deals to best suit its economic needs. However, irrespective of the trade deal the UK Government negotiates upon exit of the European Union, personal data is, and will remain, a key economic asset. Cross-border transfers of personal data will continue to underpin the UK's economy, and if the UK is to retain its position as home to the financial services industry and European base for many digital sector technology companies, and allied Fintech and data centre industries, it will have to ensure that adequate data protection measures are in place to protect the personal data of European citizens. Accordingly, UK established businesses intending to offer goods or services, including those provided free of charge, or to monitor the behavior of citizens in EEA countries should continue their Regulation (EU) 2016/679 preparedness as part of their global regulatory compliance obligations.

It is to be hoped that the UK Government will recognize the benefits of ensuring that UK data protection law is fully compliant with provisions in Regulation (EU) 2016/679, either through directly implementing its provisions, or closely mirroring them in domestic law, not least because its extraterritorial effect will make it impossible for companies that seek to establish trade relations with EU member states to ignore them. Forging its own data protection path could also lead to isolation in terms of international data protection obligations since countries that have signed and ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 are obligated to provide equivalent levels of data protection. The absence of adequate or equivalent level of data protection would impede cross-border personal data transfers, cause global business established in the UK to relocate and prompt them to reconsider future investment in the country; the antithesis of trade deal objectives.