Data protection in the UK post-Brexit: The only certainty is uncertainty

Aysem Diker Vanberg
Anglia Ruskin University, Anglia Law School, the United Kingdom

Contact : aysem.dikervanberg@anglia.ac.uk

Maelya Maunick
BPTC student at City, University of London, the United Kingdom

Keywords

Brexit, GDPR, data protection, UK

Abstract

The EU General Data Protection Regulation (GDPR) was published in the Official Journal of the European Union on 4 May 2016. The GDPR replaces the 1995 Data Protection Directive (Directive 95/46/EC). After a two-year transition period, the GDPR will be binding on all Member States including the UK, from 25 May 2018 Needles to say, the GDRP will have a profound impact on UK data protection law.

Subsequent to the referendum result on 23 June 2016 to leave the EU, the UK invoked Article 50.2 of the Treaty on European Union (TEU) and notified the EU on 29 March 2017 of its intention to withdraw from the EU.

Set against this background, this paper will critically examine the implications of Britain's exit from the EU (hereinafter Brexit) on data protection law in the UK with a particular focus on the various trade models available to the UK post-Brexit, such as the EEA model, the Swiss model, the free trade agreement adopted by Canada and the WTO model. Regardless of the agreed trade model, the GDPR will continue to be relevant for many organisations and businesses in the UK if they wish to continue operating within the EU and transferring data across borders.

This paper contends that irrespective of the model chosen for exiting the EU, the UK will adopt standards almost identical to the GDPR in order to remain a competitive

actor in the global economy. Nevertheless, even if the UK endeavours to adopt the same as or equivalent standards to the GDPR as a third country, this will not necessarily secure an adequacy decision from the European Commission potentially leading to burdensome requirements for UK businesses and their trading partners.

1. Introduction

On 23 June 2016, British citizens voted in a referendum in favour of leaving the EU by a slight majority of 51.9% (The Electoral Commission 2016). The UK invoked Article 50.2 TEU and formally notified the EU on 29 March 2017 of its intention to withdraw from the EU. Pursuant to Article 50.3 TEU, following this notification the UK has two years to negotiate a new trading relationship with the EU.[1]

As stressed in the Queen's Speech, over 70 per cent of all trade in services is enabled by data flows, and as a result data protection is crucial for the UK's international trade (HM the Queen 2017, 47). The digital sector contributed £118 billion to the UK economy and employed over 1.4 million people across the UK in 2015 (HM the Queen 2017, 47). This demonstrates that without an effective data protection framework which allows data exchanges with the EU, the UK is likely to suffer significant financial losses. As held by the Parliamentary Under-Secretary of State, Department for Digital, Culture, Media and Sport, Lord Ashton of Hyde 'some 43% of EU tech companies are based in the UK and 75% of the UK's data transfers are with EU member states' (Lord Ashton of Hyde 2017, Column 129). This shows the importance of having a smooth data transfer between the EU and the UK.

Accordingly, there is an increasing interest in the impact of Brexit on the GDPR and data protection post-Brexit in current academic literature.[2] This paper seeks to contribute to this growing body of research by analysing the implications of Brexit on data protection law under different post-Brexit trade models.

The paper is divided into six parts. Following a brief introduction, in part two, this paper will provide an overview of current data protection issues in the UK with reference to relevant case law. Subsequent to this, in part three, the paper will examine the UK Government's current position in relation to data protection and exchange of data post-Brexit. In part four, the paper will explore various trade models available to the UK post-Brexit and their implications for data protection in

the UK. The paper will assert that the EEA model appears to be the best alternative for the continuity of the GDPR but it might not materialise. In part five, the paper will discuss the conditions for securing an adequacy decision from the Commission under Article 45 of the GDPR and puts forward that even if the Data Protection Bill becomes law by May 2018, once the UK leaves the EU and becomes a third country, the UK might face issues in securing an adequacy decision from the Commission and this would lead to some burdensome administrative formalities for UK businesses. Finally, in part six some tentative conclusions will be drawn as to the future of data protection in the UK after Brexit.

2. **Current issues in UK Data Protection**

Currently in the UK, the protection of data is regulated by the Data Protection Act 1998 (DPA), which mirrors the 1995 Data Protection Directive (95/46/EC) ('EU Data Directive').[3] The data protection and privacy related articles of the EU Charter of Fundamental Rights (Articles 7 and 8) and Article 8 of the European Convention on Human Rights are also worth mentioning as they had a significant impact on shaping the data protection landscape in the UK.

In January 2012, faced with technological progress, globalisation and the discrepancies created by the inconsistent application of the EU Data Directive, the European Council recommended that a new piece of legislation, the General Data Protection Regulation (GDPR), be introduced in order to bring uniformity to the EU data protection system (Woodhouse 2017). This regulation was adopted by the EC in April 2016 and will be formally applicable within the EU on 25 May 2018 (EUGDPR.org). Unlike Directive 95/46/EC, the GDPR is a regulation so will be directly enforceable in all Member States, including the UK.

It must be noted that lately there have been concerns as to the level of data protection offered in the UK. This is because there has been a tendency to pass or attempt to pass legislations allowing extensive data sharing and surveillance powers in the interest of national security and public safety (Peers 2016). Some of those attempts failed thanks to challenges brought by NGOs or individuals. For instance, in *Secretary of State for the Home Department v. Tom Watson & others*[4] the compatibility of the Data Retention and Investigatory Powers Act 2014 (DRIPA) with the EU Charter was challenged before the Court of Justice of the European Union

(CJEU). The case was initiated in 2014 by two UK MPs, David Davis who was required to drop out of the challenge and now serves as the Secretary of State for Exiting the European Union, and Tom Watson, a labour MP. The MPs challenged the powers to require retention of certain types of data in the now repealed DRIPA. The case was later joined with a Swedish case entitled *Tele2 Sverige AB v Post-och Telestyrelsen*.[5] In the joined cases of *Tele2 Sverige and Watson*, the CJEU concluded that general and indiscriminate data retention legislation, even when it serves the objective of combating crime and terrorism, is disproportionate.[6]

Furthermore, in *Tele2 Sverige and Watson*, the Grand Chamber of CJEU ruled that DRIPA was incompatible with article 7 and 8 of the EU Charter as it amounted to extensive surveillance.[7] DRIPA was repealed on 31 December 2016 and replaced by the Investigatory Powers Act 2016 (IPA), which received Royal Assent on 29 November 2016 and became an Act of Parliament (UK Parliament, 2016). The *Tele2 Sverige and Watson* ruling is also problematic for the IPA as it largely replicates the contested provisions of DRIPA. Furthermore, arguably the IPA provides for more controversial data processing such as the retention of telecommunications data for preventing or detecting crime or preventing disorder which does not comply with the CJEU's finding in *Tele2 and Watson* (Kuşkonmaz 2017).

The IPA was not welcomed by human rights activists, civil liberties organisations or privacy experts as some its provisions are at odds with the EU Charter. As Edward Snowden tweeted on the passing of the IPA: 'The UK has just legalised the most extreme surveillance in the history of western democracy. It goes further than many autocracies.' (MacAskill 2016).

The IPA allows the interception of communications and the acquisition and retention of telecommunications data in the UK. The Act covers a wide variety of law enforcement and investigatory techniques employed by the police and the security and intelligence services, including the interception of communications data and targeted and bulk warrants. As Murray (2017, 8) puts forward, Part 4: Retention of Communications data which lists several purposes[8] that permit data retention orders to be issued is arguably much wider than the now repealed DRIPA. Murray (2017,8) also notes that in the amended version of the Act some safeguards have been added to ensure that a data retention notice is granted to the Secretary of State only

in limited circumstances and the issuance of such notices are subject to the review of the Judicial Commissioners. Under section 89 (1) of the Act, the Judicial Commissioners are entitled to review the Secretary of State's conclusions to assess whether the retention notice is necessary and proportionate for the purposes listed under Section 61(7) of the Act. However, the scope of the judicial review to be conducted by the Judicial Commissioners is rather limited as there are only three grounds to review these orders: illegality, fairness and irrationality, and proportionality (Murray 2017, 9). In other words, as put forward by Privacy International's Caroline Wilson Palow and Liberty's Director Shami Chakrabarti, such limited judicial review is not helpful and arguably not a sufficient safeguard against intrusive surveillance (HC 651 Joint Committee on the Draft Investigatory Powers Bill 2015). Despite the fact that the *Tele2 Sverige and Watson* case invalidated provisions of the now repealed DRIPA and the case does not make any reference to IPA, it is evident that the above-mentioned judgment has wider repercussions. It is submitted that the IPA, particularly Section 89 of the Act, is at odds with the above-mentioned judgment due to the extensive mass surveillance granted to UK authorities and the lack of effective safeguards within the Act that address potential misuse of the Act.

It is worth noting that in 2009 the National Council for Civil Liberties reported in one of its opinion polls that 77 per cent of the persons polled believed that the UK had become a surveillance society (Liberty 2009). Lastly, in March 2015, ten human rights organisations, following the application of the National Council for Civil Liberties, joined their claim to challenge the surveillance activities of the British Intelligence Agencies before the European Court of Human Rights (ECtHR).[9] This challenge was driven by concerns that arose from the Snowden revelations. The key issue presented before the court was whether the 'British surveillance of communications, either under its Tempora program[10] or by receipt of communications from the US government obtained in its Prism[11] or Upstream programs violated Articles 8 or 10 of the European Convention on Human Rights' (Electronic Privacy Information Centre nd.).

3. The Government's current position with reference to Brexit, data protection and the exchange of data

In various official publications and policy documents, the UK Government has continuously stated that it is fully committed to incorporating the GDPR into its data protection laws.

In its Brexit White Paper dated February 2017, the UK Government affirmed that: 'As we leave the EU, we will seek to maintain the stability of data transfer between EU Member States and the UK' (Department for Exiting the European Union and The Rt Hon David Davis MP 2017,45). Subsequently, in the Queen's Speech on June 2017 it was confirmed that the UK will introduce a new Data Protection Act which will incorporate the GDPR. The Data Protection Bill will eventually replace the Data Protection Act 1998.

In the Queen's Speech (HM the Queen 2017, 9), it was also stated that the aim of the Data Protection Bill is to ensure that the UK 'retains its world-class regime protecting personal data' with a data protection framework that is suitable for the new digital age, and to cement the UK's position at the forefront of technological innovation, international data sharing and protection of personal data. According to the Queen's Speech (HM the Queen 2017, 46) the new Data Protection Bill will contribute to the UK being in the best position to maintain its ability to share data with other EU Member States and internationally after leaving the EU. The Data Protection Bill was introduced to the House of Lords on 13 September 2017 and the first reading of the Bill in the House of Commons took place on 18 January 2018.[12] It must be noted that there might be further challenges to it before it receives Royal Assent and becomes law. The Bill has received positive comments as it brought clarity and relief to data controllers based in the UK (Kuşkonmaz 2017). Nevertheless, the Bill also has its critics. It is not a straightforward document to navigate as it constantly cross-refers to the GDPR without copying the relevant provisions of the GDPR and the language used is often complex and confusing (Hopkins 2017).

It is clear that the Data Protection Bill is intended to transpose the GDPR into UK law to ensure a smooth data transfer between the UK and the EU post-Brexit. Nevertheless, there is still no clarity as to whether this Bill would suffice to secure an adequacy decision from the EC.

On 24 August 2017, in an official document, the UK Government finally set out its plans for arrangements that could ensure that personal data would continue to move freely between the UK and the EU (Department for Digital, Culture, Media and Sport, Department for Exiting the European Union and the Rt Hon Matt Hancock MP, 2017). According to this document, after Brexit, the UK wants to explore a UK-EU model for exchanging and protecting personal data which would provide certainty for businesses, public authorities and individuals as well as enabling the UK Information Commissioner's Office and partner EU regulators to maintain effective regulatory cooperation (HM Government 2017, 2). This is indeed a welcome policy document but it is only 15 pages long and does not provide any clarity or any details as to how a UK-EU model for exchanging and protecting personal data will be formulated and negotiated. As pointed out by Antony Walker, deputy director of Tech UK, which represents a sizeable number of UK-based tech firms: 'What the Government says it wants to achieve is positive, but we urgently need more detail on how we get there, because it won't be easy or straightforward – although not impossible' (Foster 2017). Furthermore, as noted by Kuşkonmaz (2017), this document does not refer to the discussions surrounding the IPA and other potential issues including the status of EU case law post-Brexit which will still be influenced by the EU Charter.

In the light of the above, it can be said that for the time being the UK government appears to be committed and motivated to ensuring smooth data transfer between the UK and the EU and to adopting the same legal framework as the GDPR by introducing the new Data Protection Bill. Nevertheless, it must be noted that the trade models discussed below might have important repercussions on the future of the GDPR and data protection laws in the UK. For the time being, even if the UK government stays fully committed to adopting the same legal framework as the GDPR by adopting the Data Protection Bill, there will still be several complications with regard to data protection law in the UK.

Firstly, post-Brexit the decisions of EU institutions such as the EC and the CJEU will no longer be binding for the UK. This raises questions about how to resolve conflicts in relation to the application of the GDPR if the UK does not accept the authority of these institutions.

Second, even if the UK decides to adhere fully to the provisions of the GDPR and remains bound by past CJEU jurisprudence, it should be taken into consideration that UK national courts will not be subject to or able to refer cases for clarification to the CJEU, which would lead to problems and uncertainties in terms of interpretation of EU law.

Third, following Brexit UK judges would lose their power to override UK law that contravenes EU law. This was the case in *Google Inc. v. Judith Vidal-Hall & others*[13] where the UK Court of Appeal applied the EU Charter of Fundamental Rights to determine that a provision of the Data Protection Act was incompatible with EU law. Thus, EU and UK data protection laws might each be interpreted and implemented differently, resulting in the creation of discrepancies between the two judicial systems, and this could potentially lead the UK to lose its adequate level of data protection.

Finally, post-Brexit the UK would no longer be part of the European Data Protection Board (EDPR) and would have to accept decisions of the EDPR without representation, which is likely to upset those who want independence from EU institutions (Murray 2017, 3).

4. Various trade models and their implications for the future of UK data protection

The future and form of the data protection regime after Brexit depends on the trade model negotiated with the EU. This paper refers to the EEA model, the Swiss model, the Canadian model and trading with the EU as a WTO member. Other relevant models such as the Turkish Customs Union model and the Deep and Comprehensive Free Trade Agreement (DCFTA) model are not discussed in this paper as the effect of both of these models on data protection law and adequacy requirements would be very similar to the other bilateral (the Swiss and Canadian) models discussed in-depth below.

As noted by Baroness Neville Wolfe in July 2016, if the UK remains within the Single Market the EU rules on data might continue to apply fully in the UK. Nevertheless, if other trade models such as free trade agreements or the WTO model are pursued, the future of the GDPR and data protection law in the UK is rather uncertain as the UK might choose to slightly deviate from the provisions of the GDPR, which would require an adequacy decision from the Commission. This will be discussed below.

4.1 The EEA model

The UK could opt for so-called 'Soft Brexit' and join the European Free Trade Association (EFTA) whose current members: Iceland, Lichtenstein and Norway, trade with the EU in the EEA.[14] Data protection within the Internal Market has been harmonised and is part of the EEA Agreement. In other words, the above-mentioned countries will be complying with the GDPR by implementing it in their respective national system (Hasan 2016).

The UK is currently a member of the EEA through its membership of the EU. However, 'assuming the necessary agreement/approvals could be obtained (and the UK becomes an EFTA member as required under the EEA Agreement), the UK could leave the EU but join the EEA as a non-EU state member, like Norway' (Garvey 2016). The process for joining could potentially be completed in under a year, within the two-year constraint imposed under Article 50 TEU (European Union Committee 2016, 20). Other members of the EFTA would have to unanimously agree on the UK's membership beforehand. However, they may not be eager to do so (European Union Committee 2016, 20).

Moreover, if the UK joins the EEA, or enters into an equivalent agreement, it will benefit from the free movement of goods, persons, capitals and services.[15] Although the UK will benefit from the Single Market, it will be under the obligation to financially contribute to EU programmes it is taking part in as well as to the EU Regional Development Funds.[16] In a research paper entitled 'Leaving the EU' it was put forward that '[i]f the UK left the EU and instead contributed to the EU budget on the same basis as Norway, its contributions would fall by around 17%' (Miller 2013, 22). However, it must not be forgotten that one of the main reasons UK citizens voted to leave the EU was so that the UK could recover its sovereignty. By joining the EEA,

the UK will lose any influence it has over the decision-making process of any of the legislation it will have to abide by. This would lead to a dramatic loss of sovereignty compared to the power it had as an EU Member State. As Theresa May stated during the Conservative Party conference on 2 October 2016:

> We are going to be a *fully-independent*, *sovereign country*, a country that is no longer part of a political union with *supranational institutions that can override national parliaments and courts.* And that means we are going, once more, to have the freedom to *make our own decisions* on a whole host of different matters, from how we label our food to the way in which we choose to control immigration.

If the UK stays in the EEA, personal data could flow from the 27 countries and three EEA member states without any further safeguards and it would be required to fully adopt the principles in the GDPR. Furthermore, if the UK stays in the EEA, it would not need to secure an adequacy decision from the Commission. This undoubtedly constitutes the best option for the UK in terms of ensuring that data flows from the UK to the EU and visa versa remain unaffected.

Nonetheless, although this model seems appropriate for data protection and privacy in the UK, it is unlikely to satisfy the UK in its quest for sovereignty and independence so does not seem very viable for the time being. Most importantly, this trade model will require the continued influence of the CJEU, which is at odds with sovereignty and independence from the CJEU. Nevertheless, it must be noted that nothing is set in stone and that during the negotiations with the EU the UK government might change direction and reconsider the EEA agreement, or an equivalent agreement.

4.2 The Swiss model

In terms of trade models, the UK could seek to replicate the Swiss model, which is slightly different from the EEA model. Switzerland is a member of EFTA but not the EEA so its access to EU markets is governed by various bilateral agreements. Switzerland has entered into various bilateral agreements with the EU which cover insurance, education, competition law, fraud prevention, free movement and the Schengen Agreement to name a few (Swiss Confederation Directorate for European

Affairs (DEA) 2017). The advantage of the Swiss model is that it will allow the UK the flexibility to choose the EU initiatives in which it wishes to participate and the freedom to opt out of other initiatives.

Although the Swiss model seems advantageous at first glance, it has with several disadvantages. Firstly, Switzerland has no influence over the EU programmes it participates in such as Horizon 2020. More importantly, in order to secure the future of trade relations with the EU, Switzerland had to compromise on free movement of persons (Henley 2016). This makes this model unattractive for the UK, particularly due to concerns over immigration from the EU. In this regard, it is highly unlikely that the EU will provide freedom on capital, goods and services and offer a model akin to the Swiss model to the UK, without the UK accepting the free movement of people (IDS Employment Law Brief 'Brexit' 2016).

It is also worth noting that the bilateral treaties between the UK and the EU would be subject to negotiations and a unanimous agreement from the remaining EU Member States. Due to Member States taking into account their own national interests, this could be difficult to achieve within the two-year deadline provided by Article 50 TEU and potentially unrealistic for this complex process. Moreover, the EU may be reluctant to offer a preferential trade deal to the UK so as not to open the floodgates to other countries wishing to leave.

Unlike the other EEA countries, as an EFTA country Switzerland was not obligated to mirror the provisions of Directive 95/46/EC on data protection. Nevertheless, Switzerland has voluntarily mirrored the provisions of Directive 95/46/EC and received an adequacy decision from the Commission.[17] The conditions for obtaining an adequacy decision will be discussed in detail under Section 5 of this article.

As noted by McCullagh (2017,15) the degree of influence of EU data protection law on Switzerland will increase as of 25 May 2018 when the GDPR enters into force. Due to its extraterritorial application, the GDPR will apply to Swiss companies and organisations even if they have no presence in the EU as long as they process personal data of EU data subjects or monitor online behaviour of EU data subjects (McCullagh 2017,15). It must be noted that for the Commission not to revoke its adequacy decision Switzerland needed to revise the Swiss Federal Data Protection Act to reflect changes in the GDPR. The Swiss Federal Department of Justice and

Police has already revised a draft Data Protection Act in line with the GDPR. The new act is expected to come into effect in 2018 (Vermeil and Morscher 2017).

In the same vein, if the UK can replicate the Swiss model, it would be expected to align its current data protection laws with the GDPR to secure an adequacy decision from the Commission. Nevertheless, it must be noted that there would always be a risk of the Commission revoking its adequacy decision if it decided that the data protection standards in the UK were not similar or equivalent to those in the GDPR.

4.3 Free trade agreements – the Canadian model

In their Brexit White Paper (Department for Exiting the European Union and The Rt Hon David Davis MP 2017, Chapter 8), the UK Government expressed that it was not seeking membership of the Single Market but instead it wished to pursue 'an ambitious comprehensive Free Trade Agreement (FTA) with the EU'. This would allow the UK to negotiate arrangements not only for goods but also for the free movement of people.

Similar to the model adopted by Canada, the UK could negotiate a free trade agreement with the EU. The new 'Comprehensive Economic and Trade Agreement' (CETA) between Canada and the EU is described as the 'most ambitious trade agreement the EU has ever concluded' (Glossop 2016). CETA was negotiated for seven years and could have taken a further two years to ratify (IDS Employment Law Brief 'Brexit' 2016). Once approved by the European Parliament, CETA will provisionally take effect and will enable Canada's manufactured exports and 98% of its agricultural goods to be sold within the EU Internal Market without any import tariffs (McCullagh 2017, 17). The advantages of CETA for Canada are that it does not have to make any contributions to the EU budget and is not required to accept free movement of workers. At first glance, this seems like a very attractive model for the UK, given the concerns over immigration and due to the financial benefit of not having to contribute to the EU budget. As noted by Scarpetta (2016), CETA is the first third country agreement in which the EU has agreed to grant Internal Market access in the services sector other than to those sectors explicitly excluded. In other words, CETA provides access to the services sector but this access is not unlimited and it is not as extensive as enjoyed by UK companies at the moment.

Given the time it took to negotiate the CETA, it seems unfeasible for the UK and the EU to negotiate such a deep, bespoke agreement quickly enough. Hence, it is probable that the UK will encounter difficulties in coming to a desirable 'bespoke agreement' (European Union Committee 2016-2017) such as CETA.

Given the historic and geographic ties between the UK and the EU, the EU may be reluctant to offer the UK access to its markets without ensuring the continued free movement of people.

Canada currently has the Personal Information Protection and Electronic Documents Act that has similar provisions to the Directive 95/46/EC. In 2002, Canada secured an adequacy finding from the EC. It is again worth noting that this finding can be revoked by the EU at any time.

Depending on the outcome of negotiations, the UK could follow the same path as Canada with regard to data protection by seeking an adequacy decision from the Commission. Nevertheless, as mentioned above in the context of Switzerland, the Commission could always revoke its adequacy decision if it decided that the data protection standards in the UK were no longer similar or equivalent to those in the GDPR. This would create significant uncertainty for businesses in the UK and their trading partners.

4.4 Other bilateral models

Other relevant models include the Turkish Customs Union model and the DCFTA model which supports the accession process of Georgia, Moldova and Ukraine. These models are not discussed in this paper as the effect on data protection law and adequacy requirements would be equivalent to the other bilateral (Swiss and Canadian) models discussed above. Both of these models would require the UK to change its data protection law to be in line with the GDPR (which is currently being done by the adoption of the Data Protection Bill) and negotiate a bespoke bilateral agreement for the free movement of data to enable the transfer of data between EU/EEA countries and the UK.

4.5 WTO model

Another possible outcome of negotiations for the UK is a 'Hard Brexit', under which the UK fails to reach an agreement with the EU in relation to a new trading

relationship and continues to trade with the Union under World Trade Organization (WTO) rules.

The WTO was founded in 1995 and is a global framework for trade relations between countries with the aim of liberalising trade by lowering tariffs and eliminating other barriers for improved market access (European Union Committee 2016-2017, 51). It is founded upon 'agreed sets of multilateral rules which govern trade between members' (International Trade Committee 2016-2017, 8), including the General Agreement on Tariffs and Trade (GATT) and the General Agreement on Trade in Services (GATS) (International Trade Committee 2016-2017, 8).

If the UK relied on the WTO for its trading future, no contribution would be made to the EU budget and the UK would no longer be bound by the jurisdiction of the CJEU, thus allowing the UK to create agreements with third countries, which the current Government is enthusiastic to do: 'As noted in the Brexit White Paper dated February 2017, following Brexit the UK will look to increase significantly trade with the fastest growing and most dynamic export markets in the world' (Department for Exiting the European Union and The Rt Hon David Davis MP 2017, 52). Additionally, the UK would no longer have to accept the free movement of persons or comply with Single Market rules, both of which appear to have been major motivations for leaving the EU.

The process would involve the amendment of the UK's schedules with the WTO. This can be done by 'rectification' (European Union Committee 2016-2017, 53), referring to 'changes or rearrangements which do not alter the scope of concessions' (Rojas and Simpson 2017) or 'modification' (European Union Committee 2016-2017,53), referring to 'changes which do affect its scope' (Miranda and Simpson, 2017). A rectification of these schedules could be completed within 'three months' (European Union Committee 2016-2017, 53). The UK will need to 'establish new schedules … providing clarity for UK businesses' (HM Government 2017, Chapter 9.17) and would have to strike a deal on thousands of tariff lines 'covering its entire trade portfolio, to quotas on agricultural exports, subsidies to British farmers and the access to other markets that banks and other UK services companies now enjoy' (Wang, 2017). However, under the rules of the WTO, 'neither the UK nor the EU could offer each other better market access than that offered to all other WTO

members' (IDS Employment Law Brief 2016, 13-18), meaning the UK would face the Common External Tariff imposed by the EU. This would pose a significant stumbling block to this.

Reliance on the WTO rules for trade with not only the rest of the world but also the EU would lead to the most dramatic and disruptive changes to the UK. Leaving the EU would subject the UK to a significant number of restrictions and potentially affect the UK's trading patterns and, in turn, its economy.

As the WTO agreement does not cover privacy and data protection, the UK would need to acquire the 'adequate level of data protection as in the EU and secure an adequacy decision.

5. Status of data protection law in the UK post-Brexit

As noted above, the British government has announced that post-Brexit no major changes will be made to data protection law in the UK and the new Data Protection Bill will incorporate the provisions of the GDPR. However, simply adopting the Data Protection Bill might not suffice to alleviate all concerns with regard to data protection law in the UK.

5.1. Data protection and EU Charter of Fundamental Rights

On 13 November 2017, the UK Government published the first draft of the European Union Withdrawal Bill and stipulated its intention not to retain the EU Charter as part of UK domestic law on or after exit from the EU (European Union (Withdrawal) Bill, Article 5(4)). The EU Charter, particularly Article 8, plays a central role in EU law on data protection and data processing as it contains a comprehensive and free standing right to protection of personal data (Woodhouse and Lang 2017,14). The Charter gained Treaty status in 2009 and subsequent to this date many decisions including the above-mentioned *Tele2 and Watson* judgment have relied on the provisions of the Charter.

Under sections 2, 3 and 4 of the European Union Withdrawal Bill, the Government has expressed its intention to retain a majority of EU data protection legislation and case law. It is also stipulated that such law might be relied upon in domestic courts (European Union (Withdrawal) Bill, Articles 2, 3, 4).

Even though the UK will retain part of EU data protection law, one of the main concerns regarding the removal of the Charter is the ability of the UK to ensure close cooperation with the EU, given that the Charter appears to be a crucial instrument in ensuring regulatory equivalence. Further, although pre-Brexit CJEU case law will remain binding on the UK, the European Union Withdrawal Bill states that on or after exit day the UK courts and tribunals will no longer be bound by the decisions taken by the CJEU (European Union (Withdrawal) Bill, Article 6). This is problematic as it means that post-Brexit there is likely to be discrepancies between judgments in the UK and the EU. Such discrepancies might lead to confusion and have adverse repercussions on the UK securing an adequacy decision. This is discussed below in detail.

5.2 Securing an adequacy decision

If the UK leaves the EEA and becomes a third country for the purpose of data protection, it will face the same issues as other third countries like the USA, Canada and Switzerland in terms of transfer of data across borders.

According to Article 45 of the GDPR (when assessing whether a third country ensures an adequate level of protection with regard to transfer of data, the EC will consider the rule of law in force in the third country (both general and sectoral). This includes access of public authorities to personal data and the onward transfer of personal data to another third country. Furthermore, according to Article 45 of the GDPR, the Commission will consider whether an independent regulatory organisation exists in the third country and whether such an organisation is adequately equipped with assisting and advising data subjects in exercising their rights. Lastly, pursuant to Article 45(2) of the GDPR, the Commission will contemplate the international commitment of the third country in relation to the protection of personal data. An adequacy decision will be subject to periodic review, at least every four years, and such review shall take into consideration all the relevant developments in the third county in question (GDPR Article 45(3)). If, after review, the Commission considers that the third country no longer ensures an adequate level of protection, it can amend, suspend or even repeal the decision without retroactive effect (GDPR Article 45(5)).

In October 2015, in *Schrems* (Case C-362/14, 2015), the CJEU concluded that the EU-US Safe Harbour agreement, which is a special form of adequacy decision, was not valid as the USA did not meet the EU's stringent standards for adequate data protection. The case was initiated by Maximilian Schrems, an Austrian activist who was frustrated with the lack of control over his personal data that Facebook held on him as Facebook Ireland was transferring his personal data to its US servers. Schrems initially complained to the Irish Data Protection Agency and then to the Irish High Court, which referred the case to the CJEU for a preliminary ruling. Under the EU-US Safe Harbour Agreement, the US was assumed to have adequate data protection in place and as a result US companies such as Facebook could transfer data from Europe to the US. However, following Snowden's whistleblowing and revelations of mass surveillance by US intelligence agencies, the adequacy of data protection in the US was disputed. The CJEU found that the EU-US Safe Harbour Agreement which permitted transfer of data between the US and Europe was invalid as the US did not provide adequate protection to personal data, particularly with regard to safeguards against mass surveillance. As a result of this decision, the EC had to repeal its adequacy decision and negotiations have taken place between the EC and the US authorities to ensure the continuity of data transfer between two countries. On 29 February 2016, the EC presented the draft texts for a EU and US Privacy Shield Agreement and following the opinion of Article 29 Working Party and the European Parliament resolution, the EU and US Privacy Shield Agreement was adopted on 12 July 2016[18].

Unless an alternate or transitional agreement is agreed, if the UK leaves the EU and stops being part of the EEA, it needs to secure an adequacy decision from the EC as per Article 45 of the GDPR which affirms that the UK offers an adequate level of protection to personal data. The EC has so far accepted Andorra, Argentina, Canada (commercial organisations), the Faeroe Islands, Guernsey, Switzerland, Isle of Man, Jersey, New Zealand and the US as countries that provide adequate data protection and allows data transfer to them (European Commission n.d.). Pursuant to Article 45(2) of the GDPR, in order to assess the adequacy of the level of protection the Commission will take into account the rule of law, respect for human rights and fundamental freedoms, the existence of an effective and functioning independent data protection authority in the third country and the international commitments the

third country has entered into, particularly with reference to the protection of personal data.

Despite the rather positive and perhaps overly-confident statements communicated by the UK Government in various policy documents and by MPs such as Rt Hon Matt Hancock,[19] securing the adequacy decision might not be very straightforward. Arguably, the UK might have difficulties in satisfying the first limb of Article 45 2(a) of the GDPR, particularly in relation to respect for human rights and fundamental rights. As discussed above, the extensive surveillance powers in the IPA, just like its predecessor DIPRA, are likely to be seen as problematic. In particular, the ability of the intelligence agencies such as GCHQ to intercept communications data are likely to be seen at odds with EU case law such as the joined case of *Tele2 Sverige and Watson*. By giving weight to the existing case law and the EU Charter, the EC might refuse to grant an adequacy decision to the UK. Similarly, if the EC considers that the UK no longer ensures an adequate level of protection, it can repeal its adequacy decision.

5.2 Consequences of the UK failing to secure an adequacy decision

Needless to say, if an adequacy decision is not secured, this would lead to uncertainty and complexity for business and public authorities as they would not be able to freely transfer data from the UK to the EU and vice versa. In this regard, on 17 January 2018, the EC published a notice to stakeholders to address the uncertainties in data protection issues arising from Brexit (European Commission 2018). As the notice clarifies, if the UK and the EU cannot reach a transitional agreement or an adequacy decision as to the transfer of data, a controller or processor can still carry on transferring data from the EU to the UK or vice versa if they provide appropriate safeguards. These safeguards may be provided by:

i) the use of one of three sets of standard data protection clauses issued the Commission,

ii) the use of legally binding data protection rules approved by the competent data protection authority which apply within a corporate group,

iii) the use of approved codes of conduct or certification mechanisms, together with binding and enforceable commitments of the controller or processor in the third country (European Commission 2018).

The Notice also clarifies that in the absence of an adequacy decision or of the above mentioned appropriate safeguards, a transfer or a set of transfers may take place subject to certain derogations. These derogations are narrowly defined and limited to where:

i) the data subject has explicitly consented to this transfer,
ii) the transfer is necessary for the performance of a contract,
iii) the transfer is necessary for the exercise of legal claims or for reasons of public interest (European Commission 2018).

The Notice clearly shows that if the UK cannot secure an adequacy decision, UK businesses can still operate within the EU but they would be require to review their existing data protection policies and contracts thoroughly in preparation for Brexit. In other words, in the case of the UK not securing an adequacy decision, UK businesses are likely to incur significant costs to ensure that they comply with the EU requirements. Arguably, this also leads to burdensome administrative procedures for UK businesses.

6. Conclusion

As discussed above, the best option to secure the future of the GDPR and data protection law in the UK would be for the UK to remain a part of the Single Market, fully adopting the GDPR. Regrettably, at the time of writing, in the light of the Brexit White Paper (Department for Exiting the European Union and The Rt Hon David Davis MP 2017), EEA membership or other soft Brexit models such as the Swiss model do not seem like viable options for the UK. It is worth noting that the Government's position with regard to the Single Market and EEA membership can still change in the course of the negotiation process. Contrary to widely shared views, there might still be a possibility for the UK Government to change direction and stay in the Single Market, fully adopting the GDPR to ensure the smooth exchange of data.

However, in the case of a hard Brexit, despite the positive and rather optimistic picture drawn by the UK Government, the future of the GDPR and data protection laws in the UK remains unclear. There are five main reasons for this.

First, despite statements made by politicians, it is not certain that the UK government will continue to maintain similar standards to those in the GDPR post-Brexit, particularly if no trade deal has been agreed between the EU and the UK. Any significant deviation from the GDPR in the Data Protection Bill is likely to eliminate the chances of the UK securing an adequacy decision or might prompt the Commission to suspend or repeal its adequacy decision.

Second, even if the UK Government adopts standards similar or equivalent to the GDPR, there is still no clarity as to the future of the relationship between the UK and the EU. As discussed above, securing an adequacy decision from the EC could be difficult for the UK in the light of the current case law coupled with the extensive surveillance laws in the UK such as the recently introduced IPA.

Third, as the paper demonstrates, even if an adequacy decision is secured, the application and enforcement of the GDPR standards in the UK will be very complicated given that the decisions of EU institutions such as the CJEU will no longer be binding for the UK. As highlighted by Murray, no longer a Member of the EDPR and having no influence over its decisions, the UK would still need to comply with the decisions of the EDPR post-Brexit, which is likely to be very upsetting for those who want a complete separation from the EU (Murray 2017, 3).

Fourth, as discussed above, in the absence of an adequacy decision UK businesses with links to the EU will need to thoroughly review their existing data protection policies and contracts. This would arguably be a significant administrative burden for UK businesses.

Finally, even if the UK manages to secure an adequacy decision from the Commission, it is worth noting that the Commission can suspend or even repeal its decision at any time if it believes that the UK no longer ensures an adequate level of data protection. This uncertainty and unpredictability might push digital companies to move their operations outside the UK. This would indeed lead to dire consequences for the UK economy.

As the title of the paper suggests, no one can say with clarity what the future holds for UK data protection law in the aftermath of Brexit. The one thing that can be said with certainty is that the future of the GDPR and the data protection regime in the UK is uncertain and, in the case of a hard Brexit, it will continue to be so.

Notes

1. Article 50.3. Treaty on European Union asserts:
The Treaties shall cease to apply to the State in question from the date of entry into force of the withdrawal agreement or, failing that, two years after the notification referred to in paragraph 2, unless the European Council, in agreement with the Member State concerned, unanimously decides to extend this period.

2. There are indeed several well-written articles on Brexit and data protection. For an extensive discussion of the status of data transfers between the EU and the UK see e.g. (Murray, 2017); (de Hert and Papakonstantinou, 2017); (Moerel and Tigner, 2016); (McCullagh, 2017).

3. European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJL 281/31. This directive has been complemented by other legal instruments such as the E-Privacy Directive.

4. Home Department v. Tom Watson & others, Case-698/15.

5. See joined Cases C-203/15 and C-698/15, 21 December 2016, ECLI: EU: C: 2016:970.

6. See joined Cases C-203/15 and C-698/15, 21 December 2016, ECLI: EU: C: 2016:970 para.112.

7. Ibid para. 125.

8. The list of permitted purposes for data retention notices are found in Section 61(7). New permitted purposes include; to assist investigations into alleged miscarriages of justice, to assist in the identification of a person or their next of kin and functions relating to the regulation of financial services and markets or financial stability.

9. A copy of the application of 10 NGO's can be accessed online. Accessed January 23, 2018. https://privacyinternational.org/sites/default/files/HR%20Orgs%20v%20UK.pdf.

10.Tempora is a program under which the Government Communications Headquarter (GCHQ) has placed data interceptor on transatlantic fibre-optic cable, which allows the agency to gather information and intelligence in and out of the UK.

11. Prism is a US programme, operated by the National Security Agency and which collects Internet data ranging from emails, files and photos to data from companies such as Google, Yahoo and Facebook.

12.See stages for the Data Protection Bill
https://services.parliament.uk/bills/2017-19/dataprotection/stages.html.

13.*Google Inc. v. Judith Vidal-Hall & others* [2015] EWCA Civ 311.

14.The EEA Agreement was established by a series of agreements signed in 1992. The agreement allows Lichtenstein, Norway and Iceland to largely participate to the EU's Internal Market.

15. See EFTA, EEA Agreement (*EFTA*) <http://www.efta.int/eea/eea-agreement> accessed January 23, 2018.

16. Europa, 'European Regional Development Fund' (*Europa*) Accessed January 23, 2018. http://ec.europa.eu/regional_policy/en/funding/erdf/

17. See 2000/518/EC Commission Decision of 26 July 2006 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).

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

19.When asked for the default position if the UK does not secure an adequacy decision from the Commission, the Rt Hon Matt Hancock stated that: 'We are seeking unhindered data flows, and that we are confident we will achieve it'. This seems like a very confident statement. See the Rt Hon Matt Hancock, evidence to the EU Home Affairs Sub-Committee February 1, 2017 http://www.parliamentlive.tv/Event/Index/b3334d4c-93bf-4aca-9df5-666b7a72c06c.

References

de Hert, Paul and Vagelis Papakonstantinou. 2017. The rich contribution to the field of EU data protection: Let's not go for 'third country status' after Brexit. *Computer Law and Security Review* 33, no 3: 354-360.

Department for Exiting the European Union and The Rt Hon David Davis MP. 2017. "The United Kingdom's exit from and new partnership with the European Union White Paper." Accessed January 23, 2018. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/589191/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Web.pdf.

Electronic Privacy Information Centre. "10 Human Rights Organisations v. UK' (*Epic*) "Accessed January 23,2018. https://epic.org/amicus/echr/liberty-gchq/.

European Commission. nd. " Adequacy Of The Protection Of Personal Data In Non-EU Countries." Accessed 23 January 2018. https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en#dataprotectionincountriesoutsidetheeu.

European Commission. 2018. "Notice to Stakeholders Withdrawal of the United Kingdom from the Union and EU Rules in the Field of Data Protection." Accessed January 23, 2018 http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=607669

European Union Committee. 2016-2017. "*'Brexit: The Options for Trade* (5th Report) HL paper 72 ." Accessed January 23,2018 https://www.publications.parliament.uk/pa/ld201617/ldselect/ldeucom/72/72.pdf.

Foster, Peter. 2017. " UK Government Will Seek To Remain Fully Involved In Shaping EU Data Protection Regulations Post-Brexit." Telegraph, August 24. http://www.telegraph.co.uk/business/2017/08/24/uk-government-will-seek-remain-fully-involved-shaping-eu-data/.

Garvey, Sarah. 2016. "Analysis – Brexit: the legal mechanisms for a UK exit from the EU." *Tax Journal* issue 1315, 20.

Glossop, Peter. 2016. "Canada-EU Free Trade Agreement." *Int. T.L.R*. 22(4) no.3.

Hasan, Ibrahim. 2016. "Data protection and Brexit." *The Law Society Gazette* https://www.lawgazette.co.uk/legal-updates/data-protection-and-brexit/5057412.article

HC 651 Joint Committee on the Draft Investigatory Powers Bill. "HC 651 Joint Committee on the Draft Investigatory Powers Bill, Oral evidence." 2015. Accessed January 23, 2018. https://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/oral-evidence-draft-investigatory-powers-committee.pdf.

Henley, John. 2016. "Switzerland Makes U-turn Over EU Worker Quotas To Keep Single Market Access." The Guardian, December 16. https://www.theguardian.com/world/2016/dec/16/switzerland-u-turn-quotas-on-eu-workers-immigration.

HM Government. 2017. "The Exchange And Protection Of Personal Data: A Future Of Partnership Paper." Accessed January 23, 2018. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf.

HM The Queen, June 2017. "The Queens Speech." Accessed January 23, 2018. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/620838/Queens_speech_2017_background_notes.pdf.

Hopkins, Robin. 2017. " The Data Protection Bill: a Brief Overview." Last modified September 25, 2017. https://uk.practicallaw.thomsonreuters.com/w-010-5346?transitionType=Default&bhcp=1&contextData=(sc.Default).

IDS Employment Law Brief. 2016. *Brexit - the UK's future relationship with the EU.* IDS Emp. L. Brief.

International Trade Committee. 2016-2017. "UK Trade Options Beyond 2019 (1st Report, Session 2016-17), HC paper 817." Accessed January 23, 2018. https://www.publications.parliament.uk/pa/cm201617/cmselect/cmintrade/817/81702.htm.

Kuşkonmaz, Elif Mendos. 2017. "Brexit and Data Protection: The Tale of Data Protection Bill and UK-EU Data Transfers". EU Law Analysis (blog) September 26. http://eulawanalysis.blogspot.co.uk/2017/09/brexit-and-data-protection-tale-of-data.html.

Lord Ashton of Hyde. 2017. " Data Protection Bill House of Lords second reading." Accessed January 23, 2018. https://hansard.parliament.uk/lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/Debate.

Liberty. 2009. "Another Home Secretary; another ID card launch - as public support for the scheme sinks." Accessed January 23, 2018. https://www.liberty-human-rights.org.uk/news/press-releases/another-home-secretary-another-id-card-launch-public-support-scheme-sinks.

MacAskill, Ewen. 2016 ' Extreme surveillance becomes UK law with barely a whimper.' The Guardian, November 19. <https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper>

McCullagh, Karen. 2017. Brexit: Potential Trade And Data Implications For Digital And 'Fintech' Industries. *International Data Privacy Law* 7, no.1: 3-21.

Miller, Vaughne. 2013. "Leaving the EU." *House of Commons Research* Paper 13/42.

Moerel Lokke and Ronan Tigner. 2016. "Data Protection Implications of Brexit." *European Data Protection Law Review* 2, no. 3 : 381-383. https://doi.org/10.21552/EDPL/2016/3/14

Murray, Andrew D. 2017. "Data transfers between the EU and UK post Brexit?". *International Data Privacy Law* 7 (no. 3, August 1) https://doi.org/10.1093/idpl/ipx015 (accessed January 23, 2018)

Neville- Rolfe, Lucy. 2016. "The EU Data Protection Package: The UK Government's Perspective.'" Accessed January 23, 2017. https://www.gov.uk/government/speeches/the-eu-data-protection-package-the-uk-governments-perspective.

Parliament. 2016. “Investigatory Power Act 2016.” Accessed January 23, 2018. http://services.parliament.uk/bills/2015-16/investigatorypowers.html

Peers, Steve. 2016. “ How would Brexit affect data protection, privacy and surveillance laws in Britain?” Inforrm’s (blog) May 11. https://inforrm.wordpress.com/2016/05/11/how-would-brexit-affect-data-protection-privacy-and-surveillance-laws-in-britain-steve-peers/.

Prime Minister Theresa May. 2016. “Theresa May - her full Brexit speech to Conservative conference.” Independent, October 2. http://www.independent.co.uk/news/uk/politics/theresa-may-conference-speech-article-50-brexit-eu-a7341926.html.

Rojas, Milagros Miranda and Mark Simpson. 2017. “ The UK retaking its membership in the WTO.” Norton Rose Fulbright Inside Brexit (blog) , February 24. http://www.insidebrexitlaw.com/blog/the-uk-retaking-its-membership-in-the-wto.

Scarpetta, Vincenzo. 2016. “What could EU- Canada Free Trade Deal Tell Us About Brexit.” Open Europe. Accessed January 23, 2018. http://openeurope.org.uk/today/blog/what-could-the-eu-canada-free-trade-deal-tell-us-about-brexit/

Swiss Confederation Directorate for European Affairs (DEA)“The major bilateral agreements Switzerland–EU. Presentation by Swiss Confederation Directorate for European Affairs DEA. 2017”. Accessed January 23, 2018. https://www.eda.admin.ch/content/dam/dea/en/documents/folien/Folien-Abkommen_en.pdf

The Electoral Commission “EU Referendum Results.” Accessed January 23, 2018 http://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information.

The European Parliament and The European Council. Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L 119/1.

Vermeil, Guy and Lukas Morscher. 2017. “Revision of Swiss Federal Data Protection Act.” Lexology. Accessed January 23, 2018. https://www.lexology.com/library/detail.aspx?g=8b8a8e81-97fb-47c7-8921-dc7e108b0b63>

Wang, Ping. 2017. “Brexit and the WTO Agreement on Government Procurement *“(GPA)*. P.P.L.R. 1, 34-61

Woodhouse, John and Arabella Lang. 2017. “Brexit and Data Protection” Briefing Paper Number 7838.