International Interdisciplinary Business-Economics Advancement Journal
ISSN 2375-9615 (online)
ISSN 2375-9607 (print)
IIBA Journal, vol. 3, no. 1, pp. 29-40, February 2018

Brexit's Effect on the UK's Data Privacy Policy and the EU Privacy Shield

Margaret E. Vroman[1] and Carol W. Johnson[2]

College of Business
Northern Michigan University, USA
[1]mvroman@nmu.edu
[2]carjohns@nmu.edu

Abstract

Today's business is dependent on information; information about an individual's financial wealth, education, purchasing preferences and even health conditions. How companies treat the information, or data, they accumulate from individuals is governed by the laws in which they are incorporated and operate. Unfortunately, these laws often conflict especially when an American business is operating in Europe. This conflict led the European Commission to develop data privacy principles known as the Safe Harbor Directive, which if followed allowed US companies to store and use EU customer data. However, a lawsuit challenging the legitimacy of the Safe Harbor's privacy protections for EU citizens resulted in a 2015 ruling by the European Court of Justice (ECJ) that invalidated the Safe Harbor Directive. The chaos that resulted from this ruling sent businesses on both sides of the Atlantic scrambling for an alternative. Unfortunately, Brexit has made an extremely complex legal and business situation even more complicated. Brexit raises two important questions concerning the EU's recent invalidation of the Safe Harbor Directive that this paper will address: 1) what impact will the UK's decision to leave the EU have on the newly enacted Privacy Shield and 2) what data privacy measures will the UK implement when it is no longer part of the EU?

Keywords: Brexit, Safe Harbor, Privacy Shield, data, privacy, GDPR

Background

The ECJ's ruling that invalidated the Safe Harbor agreement, under which American and European enterprises had been operating since 2000, was handed down in 2015 (The High Court of Ireland, 2015). The rationale for the court's conclusion was that the Directive's provisions did not sufficiently protect European data in the United States (The High Court of Ireland, 2015). Its immediate impact was felt by more than 4,400 US and European companies that relied on it to transfer data back and forth in support of both trade and jobs (Nakashima, 2015). But the elimination of the Safe Harbor agreement also had huge consequences for US intelligence

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

agencies, which depend on large volumes of international data in their perpetual search for clues to disrupt terrorist plots (Nakashima, 2015).

The situation that gave rise to this precedent setting case arose when an Austrian citizen and Facebook user, Max Schrems, filed a complaint with the Irish data protection commissioner alleging that his Facebook data, which was transferred from Facebook's Irish subsidiary to servers in the United States, was inadequately protected (Price, 2015). He based his claims on news reports that described US government surveillance of personal data as revealed in documents leaked by a former US government contractor, Edward Snowden (Price, 2015).

Schrems's complaint was rejected by the Irish commissioner who cited a European Commission decision from 2000, which determined that the United States, under the Safe Harbor agreement, ensures the privacy of data that is transferred to certified companies (Nakashima, 2015). However, on review, the Irish High Court referred the case to the European Court of Justice (ECJ) on the question of whether a national data-protection authority is bound by the commission's finding. On this question the ECJ's advocate general issued an advisory opinion, which concluded that national privacy authorities are not bound by the commission's decision. The advocate general also concluded that the Safe Harbor provision itself lacked adequate privacy protections for transferred data (Nakashima, 2015).

The importance of this ruling was twofold: First, it allowed each data protection authority to examine whether a transfer of data complied with European privacy rules, and to raise the issue with its national court if it believed it did not, and it could have its national court refer the issue to the ECJ for a ruling (Weiss & Archick, 2016).

Second, it ruled the Safe Harbor agreement, under which the EU and the United States had been operating for 15 years, invalid. Its rationale for this finding was that the Safe Harbor placed "national security, public interest or law enforcement requirements" over privacy principles (Nakashima, 2015).

The court went on to say that in agreeing to Safe Harbor in 2000, the European Commission erred by not determining whether U.S. law provided adequate privacy protection for Europeans (Nakashima, 2015).

The immediate result of this ruling was that businesses that had been relying on the Safe Harbor agreement to transfer data had to seek alternate data transfer measures. Thousands of trade and investment relationships depended on it. According to a 2014 study, cross-border data flows between the United States and Europe are the highest in the world and 50% higher than data flows between the United States and Asia (Meltzer, 2014). For the short term, businesses began using a range of alternative mechanisms to govern personal data transfers including contractual clauses and binding corporate rules.

It was not just businesses that were concerned about the impact of this ruling, governments too began scrambling to find a replacement mechanism and on February 2, 2016 officials from both continents announced an agreement "in principle", which they referred to as the Privacy Shield. Almost immediately, however, critics began to assail this agreement by saying it was not strong enough to withstand future legal challenges. Even so, many U.S. policymakers and trade groups

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

believe the recently concluded U.S.-EU "umbrella" Data Privacy and Protection Agreement (DPPA), which seeks to better protect personal information exchanged in a law enforcement context, and the newly enacted U.S. Judicial Redress Act, which extends the core of the judicial redress provisions in the U.S. Privacy Act of 1974 to EU citizens, will ease enough of Europe's concerns about U.S. data protection standards to boost confidence in the Privacy Shield (Weiss & Archick, 2016).

The problem of how to handle transatlantic data transmission was exacerbated by Brexit since a new layer of complexity has been added since the UK must now determine whether it will follow the EU privacy shield rules or some other scenario.

As the second largest economy in Europe after Germany, and one that is extremely data dependent, the UK must quickly resolve this issue since its economy cannot afford the consequences of indecision. Obviously, if it had stayed part of the EU, the UK would be bound by any data transfer agreements worked out between the EU and other governments but now that it has voted to remove itself from Europe, what are the data transfer requirements that it and its foreign business partners are obligated to follow?

As of May 29, 2017, when Britain officially triggered Article 50 of the Treaty of Lisbon, the UK will have two years to negotiate its withdrawal from the EU (Wilkerson & Midgley, 2017). During this time, existing EU legal agreements remain in effect and the UK must continue to abide by EU treaties and laws even though it may not take part in any decision-making processes of the EU (Mason, Asthana, Rankin, & Boffey, 2017). How the actual exit from the European Union will be accomplished involves layers upon layers of political, economic and social considerations and negotiations. Already UBS and HBSC, two if Britain's largest financial institutions, have decided they cannot wait to see how the country deals with the requirements of the EU's data privacy and transfer requirements and they have announced their decisions to relocate (Batchelor, 2017) and according to one article up to 40% of US firms with British offices are considering relocating to the EU (Rodionova, 2016).

Looking forward, what do the people with political and business experience foresee the effect of Brexit being on data dependent industries? Their predictions will be discussed below.

The UK's Possibilities According to the Experts

Views From Within the UK

Naturally, British officials want to downplay any perception that Brexit will leave a legal vacuum that makes is unsafe for data dependent businesses to operate. Therefore, immediately after the Brexit vote the UK Information Commissioner's Office (ICO) issued a statement attempting to reassure parties that the UK's Data Protection Act of 1998 "remains the law of the land irrespective of the referendum result" (McLellan & Felz, para.4, 2016).

That said, however, Baroness Neville-Rolfe, the UK minister responsible for data protection, acknowledged that the UK's decision to leave the EU means that "for a period the future will be more uncertain" and it is not certain if the (EU's) General Data Protection Regulation (GDPR) will apply in the UK. "We do not know how closely the UK will be involved with the EU system in

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

future," Neville-Rolfe said. "On one hand if the UK remains within the single market EU, rules on data might continue to apply fully in the UK. On other scenarios we will need to replace all EU rules with national ones. She also put forth the possibility that the UK could agree to a parallel Privacy Shield directly with the US" (Out-Law, 2016, para. 13).

Another political insider, the former information commissioner of the UK, Christopher Graham, is also on record as saying that UK data protection laws need to be updated regardless of whether the GDPR regulations are adopted in the country (Out-Law, 2016). However, as a practical matter, he believes it is almost certain that the UK will end up abiding by them, at least temporarily, due to the time it will take the country to withdraw from the EU.

So far, most of the voices coming out of Britain seem to be carrying the message of "keep calm and carry on" when dealing with Brexit's effect on data transfer policies. However, that does not seem to be the perspective shared by others who must deal with a newly liberated United Kingdom.

Views From Outside the UK

The predictions for the United Kingdom's post Brexit future from outside the island nation do not seem to be as optimistic as those proffered by British officials.

Although most experts agree that Brexit will not affect the Privacy Shield agreement, serious concerns by industry experts are being expressed for the combined effect of Brexit and the lack of a coherent privacy protection policy. Chris Jeffery, head of UK IT, Telecoms and Competition at law firm Taylor Wessing, says: "The uncertainty as to whether the U.K. will be considered safe for data flows relating to citizens from the rest of Europe is causing concern, and making some companies consider whether data center capacity in mainland Europe is the safer bet" (Crabtree, 2016, para. 2).

American business executives have also expressed concern that "Leaving the EU could impede the U.K.'s free movement of data to and from the continent, negatively impacting businesses." This stems from the UK and EU's potential divergence in data protection laws post-Brexit (Kovacs, 2015). Furthermore, Post-Brexit, the UK could find itself in the situation of having to demonstrate "essential equivalence" in terms of protecting privacy, according to experts at the Global Privacy Summit in Washington (Kovacs, 2015).

Dutch member of European Parliament Sophie In't Veld, who is active on EU data protection laws, has also pointed out problems with the UK's surveillance laws. "We have to bear in mind that mass surveillance was a key issue in the European Court of Justice ruling [striking down Safe Harbor]," she said (Baker, 2016). "The activities of the British intelligence and law enforcement services do not appear at first sight to be substantially more in line with the standards set by the court. So that would probably be very problematic for the UK. Not just for trade, but also for law enforcement and intelligence" (Baker, 2016, para. 16).

Some US executives are concerned that the lack of a definitive legal system for the handling of UK and EU data may result in expensive data transfer operations. Such uncertainty would force many companies to face an unpleasant choice between risking major fines for noncompliance or pulling out of Europe. While firms could, in theory, store the data entirely in Europe, doing so is

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

often impractical or too expensive. Antony Walker, deputy CEO of industry body techUK explains that the U.K.'s service-based economy means that the transfer of data across borders is fundamental and affects industries from automotives to financial services (Crabtree, 2016). Another industry executive, Chris Jeffery, head of UK IT, Telecoms and Competition, says Brexit is responsible for "The uncertainty as to whether the U.K. will be considered safe for data flows relating to citizens from the rest of Europe is causing concern, and making some companies consider whether data center capacity in mainland Europe is the safer bet" (Crabtree, 2016, para. 2).

It is also important to note that even if the overlap between the UK's EU membership and the application of the GDPR in the UK were to be short lived, any UK business which trades in the EU will have to comply with the GDPR despite Brexit taking effect. That's because the GDPR's many obligations will apply to organizations located anywhere in the world which process EU citizen's personal data in connection with their offer of goods or services, or their "monitoring" activities. Also, any UK business that has operations within the EU will have to comply with the GDPR's provisions. It will also have to abide by the amendments to the e-Privacy Directive when they become finalized. If the UK were to decide not to upgrade its data protection laws to a GDPR level standard, the question after the GDPR's 25th May 2018 implementation will be whether the UK laws offer data protection 'adequacy' for EU citizens. The answer to that will almost certainly be that they do not. That will put the UK in the position of having to adopt either stronger EU data protection laws or create its own EC approved data transfer mechanism (as the US has done with the Privacy Shield).

According to a survey undertaken by Ovum, a global analyst firm, two-thirds of global companies plan to review their business strategies in European countries as a result of the General Data Protection Regulations (GDPR) (Ashford, 2015). This same survey revealed that 68% of respondents believe the new regulations will dramatically increase their costs of doing business in Europe, and over 50% feel they will not be able to fulfil the requirements set out by the EU (Baker, 2016). 58% of US respondents belied that the new rules will make fines for them inevitable and 70% of all respondents believe that the new rules favor European businesses (Baker, 2016). Given this, what is the likelihood that the privacy shield and its progeny will be successful?

What Does the Data Shield Require and How Does It Differ From the Safe Harbor?

The EU-US Privacy Shield addresses the failings pointed out by the European Court of Justice in its ruling on 6 October 2015, which declared the Safe Harbor framework invalid. According to its proponents, the new arrangement will mandate stronger obligations on companies in the US to protect the personal data of Europeans and require stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission (FTC) as well as increased cooperation with European Data Protection Authorities. The new arrangement includes commitments by the US that those who access personal data transferred to the US under the privacy shield will be subject to clear conditions, limitations and oversight, which will prevent generalized access. Europeans will have the opportunity to raise inquiries or complaints before a newly established Ombudsperson.

The following is a short summary of the main elements of the new Privacy Shield regulations:

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

Requirements for Companies That Handle Personal Data - With Enforcement Mechanisms

US companies that want to import personal data from Europe must commit to robust obligations on how personal data is processed and individual rights are guaranteed. The Department of Commerce will ensure that companies publish their commitments, which makes them enforceable under US law by the US Federal Trade Commission (FTC). Also, any company that handles human resources data from Europe must agree to comply with decisions by European DPAs (European Commission Press Release, 2016).

Safeguards and Transparency Obligations on U.S Government Access

For the first time, the US has given the EU written assurances that the access of public authorities for law enforcement and national security purposes will be subject to clear limitations, safeguards and oversight. Exceptions must be used only to the extent necessary and proportionate. The US has ruled out indiscriminate mass surveillance on personal data transferred to the US under the privacy shield. As part of the monitoring process there will be an annual joint review, which will also include the issue of national security access. The European Commission and the US Department of Commerce will conduct the review and invite national intelligence experts from both the US and European Data Protection Authorities to it (European Commission Press Release, 2016).

Effective Protection of EU Citizens' Rights With Several Redress Options

Any citizen who considers that their data has been misused under the privacy shield will have several redress options. Companies have deadlines to reply to citizen complaints. European DPAs can refer complaints to the Department of Commerce and the Federal Trade Commission. In addition, Alternative Dispute resolution will be free of charge. For complaints on possible access by national intelligence authorities, a new Ombudsperson has been created (European Commission Press Release, 2016).

In addition, the revised draft addresses concerns voiced by the European Parliament, Article 29 Working Party, and European Data Protection Supervisor. It includes measures dealing with:

Bulk Data Collection

The U.S. will provide further details on its bulk data collection practices, specifying the preconditions for "targeted and focused" personal data collection and safeguards for how the data may be used.

US Ombudsperson to Address Complaints

A U.S. Ombudsperson will address complaints regarding the U.S. government's use of EU citizens' personal data. The Ombudsperson will be independent from U.S. national security services.

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

Data Retention Restraints

More explicit data retention restraints, requiring that personal data be deleted when it no longer serves the purpose for which it was collected.

On paper, the EU-US Privacy Shield's protections are stronger than Safe Harbor's. There are clear safeguards on how U.S. government and law enforcement agencies can access European consumers' personal information, and it will also be easier and cheaper for people to file complaints against companies for perceived privacy violations. Also, under the "onward-transfer" provision, third-party contractors such as email-list processors that handle customer data must also adhere to the framework's principles.

On July 25, 2016, the European Commission published rules associated with the Privacy Shield agreement, along with a citizen, which provides information to EU consumers concerning how they can file complaints about the handling of their data by US companies. With the enactment of the EU-US Privacy Shield data transfer agreement, US businesses can start signing up for and begin implementing its data privacy principles on August 1, 2016. This will finally put an end to the legal no man's land under which they have been operating since October 2015 when the Safe Harbor was declared invalid. Of course, if its mechanisms are found lacking, European officials can invalidate this agreement too and it will once again be a patchwork of uncertainty.

Will the Privacy Shield Survive?

Although businesses are hopeful the privacy shield will resolve the problems identified in the Safe Harbor and provide the stability needed for business and government data transfers quite a few civil liberty groups, on both sides of the Atlantic, remain critical complaining that that there are no meaningful protections for European consumers against mass surveillance by the US government. This appears to be exacerbated by the newly elected American administration (American Civil Liberties Union, 2017). Ironically, Brexit may make it less likely that the new privacy shield will be struck down since judges and regulators may be loath to add to the economic uncertainty already and angst that it has created.

For its part, the European Commission not only claims to have improved the Safe Harbor agreement in the Privacy Shield by making it more business friendly and easier for US multinationals to legally process the personal data of EU employees and customers through a reduction of EU red tape concerning data transfer, while at the same time claiming the privacy shield's data protection measures are stronger and its enforcement mechanisms more robust, it believes this new arrangement will survive the inevitable legal scrutiny it will receive (Meyer, 2016).

Obviously, to be successful the privacy shield must be adopted by industry and so far, some important industry leaders, such as Microsoft and Google, have indicated they are interested in adopting the Privacy Shield (Eriksson, 2016).

However, the person who initiated the lawsuit that struck down the Safe Harbor agreement, Max Schrems, thinks a legal challenge to the privacy shield will succeed in destroying it as well (Eriksson, 2016). Schrems said the privacy shield agreement fails to address the ECJ's concerns

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

and is full of loopholes. He maintains that US authorities can still access EU citizens' data on very thin grounds and that although the ECJ insisted on better access to justice, the new deal has limited redress mechanisms to a toothless ombudsman (Eriksson, 2016). It is clear, he claims, that the Safe Harbor's replacement does not require the US to offer a level of protection "essentially equivalent" to that of the EU (Eriksson, 2016).

What Data Privacy Rules Will the UK Follow When It Completes Brexit?

After the Brexit vote, the UK Information Commissioner's Office (ICO) made it clear in its press release of June 24, 2016, that the Data Protection Act of 1998 (DPA) remains the law of the land and all processing of personal data must be undertaken in accordance with it. However, more recent statements confirmed that data protection law reform is necessary although the precise form it will take is unclear (Massey, 2016).

The DPA allows personal data to be transferred freely to the European Economic Area (EEA) member states and those countries covered by European Commission findings of adequacy. It also provides that consent, model clauses, binding corporate rules (BCRs) and self-assessed adequacy may be used to legitimize international transfers of personal data to countries outside the EEA, which are not covered by an adequacy decision. In addition, although the Safe Harbor framework is no longer a valid means for legitimizing data transfers to the US, the ICO's position remains that it "… will not be seeking to expedite complaints about Safe Harbor while the process to finalize its replacement remains ongoing and businesses await the outcome" (Massey, 2016, para. 6).

That is somewhat reassuring for businesses in the short term but what are the UK's options for data privacy agreements once Brexit takes effect? Experts have offered a number of possibilities.

The UK's Options

Implement the GDPR (or its Equivalent)

Following its exit from the EU, the U.K. may decide to implement the GDPR and repeal the DPA through national legislation. This option would help facilitate trade links with the EU. If the UK remains outside the EEA but implements the GDPR, or something very similar, then it is likely that the European Commission would issue a finding of adequacy.

Use the Norwegian Model (The European Free Trade Association (EFTA) Model)

Often referred to as the Norwegian model, the UK could remain a party to the European Economic Area (EEA) Agreement, which would allow it to benefit from free trade arrangements and be included in the EU single market. But it will also have to commit to comply with certain fundamental EU rules and restrictions (which may defeat part of the reason for voting to leave the EU). For Norway, Iceland and Lichtenstein (the existing non-EU members of the EEA) this currently means that they have each implemented the Data Protection Directive and the e-Privacy Directive into their respective local laws. It seems unlikely that the UK will be able to avoid accepting the GDPR if this option is adopted (Mullock and Shooter, 2016). Under this option, data transfers from the UK across the EEA would be permitted freely and the UK would benefit

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

from the European Commission's findings of adequacy in respect of protection for personal data. The UK (along with all other EEA Member States) would also be able to avail itself of the protections offered by the proposed EU-US Privacy Shield regarding personal data transfers to the US (Massey, 2016).

Just Be "Adequate"

If the UK were to leave the EU and not become a member of the EEA, it would be treated as a third country by the EU for the purposes of international personal data transfers. As stated above, if the UK chose to implement a new regime based on the GDPR principles it is likely that the Commission would find the protection afforded to personal data by the UK to be adequate and add the UK to its "white-list," of approved countries under Data Protection Directive (95/46/EU). However, if the UK were to retain the DPA and not implement an equivalent to the GDPR, then it is possible that no finding of adequacy would be made on the grounds that the GDPR is more robust in its protection and requirements than the Directive (and therefore the DPA). Furthermore, some may view the UK's historical interpretation, implementation and pragmatic approach in respect of the Directive as offering a lower standard of protection than that which will be required under the GDPR. In this scenario, all personal data transfers to the UK from the EEA would need to be legitimized by model clauses, BCRs, consent or any of the other safeguards or derogations available under the GDPR, with the U.K. controller or processor being the data importer in each case. This would likely require many organizations to review the commercial contracts and data sharing arrangements that are currently in place to ensure ongoing compliance (Massey, 2016).

Create a EU-U.K. Privacy Shield

If the UK decided to remain outside the EEA and not implement the GDPR, and instead decided to rely on the DPA, such a regime would likely be deemed insufficient for a Commission adequacy finding under the GDPR. In addition, the Investigatory Powers Bill (IPB), which is currently before the UK Parliament, may make a finding of adequacy even less likely. This is because, as currently proposed, the IPB would allow bulk personal datasets to be collected for purposes of national security without regard to data protection compliance (Massey, 2016).

In the absence of an adequacy finding by the Commission, one possibility would be to implement a "Privacy Shield" type arrangement between the UK and the EU similar to the proposed EU-US Privacy Shield. However, the proposed terms of the IPB may mean that the UK will find itself in a similar position to the one that the US is in at present. There would need to be careful negotiations as to the form of arrangement allowing for international data flows to the UK (Massey, 2016).

Create a Dual System

There is another option in which the DPA remains in force and is applied to all international data flows from the UK outside the EEA when a controller is established in the UK. In such instances the processing of personal data takes place exclusively in the UK and the processing is limited to UK citizens. For all other international transfers the GDPR would apply. Among other things, this could allow the UK to assist small businesses. However, the complexity of administration of this proposal makes it a very impractical solution (Massey, 2016).

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

Use the Swiss Model

Switzerland is not a member of the EEA, but is a member of the EFTA. It accesses the EU single market via a regularly updated bilateral agreement. Switzerland has its own data protection laws which look and feel very similar to the laws of an EU Member State that has implemented the Data Protection Directive. Indeed, Switzerland's laws have been recognized as "adequate" by the European Commission (EC) – i.e. adequately protective of the rights of EU citizens thereby enabling transfers of personal data from EU data controllers to Swiss based importers to legitimately take place. It remains to be seen whether, when and how Switzerland will update its current data protection laws to mirror the GDPR to ensure that its 'adequacy' decision is not revoked by the EC after the GDPR comes into force, although the Swiss government has already indicated its intention to seek to retain its adequacy status after May 2018. The UK would face the same decision in relation to GDPR adoption were it to adopt a Swiss style relationship with the EU (Mullock & Shooter, 2016).

Go It Alone

It is also possible that the UK might seek to strike deals with the EU independently or via collective organizations, such as the WTO (i.e. following the approach currently adopted by countries such as Canada and the USA.) If it does, then it will have free rein to choose the form of data protection laws that it introduces to update the DPA. However, recent history tells us that when it comes to the question of data transfers, EU regulators and courts take an extremely dim view of countries that do not adopt EU-strength data protection laws. The current stand-off with the US concerning the now invalid Safe Harbor data sharing arrangement proves this point. The UK economy, especially its financial services sector, relies on an ability to transfer data freely to and from the UK and cannot afford a miscalculation (Mullock & Shooter, 2016).

Other Options

Britain has other options, but they are hardly more palatable. Of course, its options also depend on the European Union which might decline to strike any deal, thus creating uncertainty in Britain and around the world. In a meeting between the United States Treasury secretary, Jacob J. Lew, and the chancellor of the Exchequer, George Osborne, Mr. Lew urged that both sides demonstrate "flexibility" in their discussions. "A highly integrated relationship between the E.U. and the U.K. is in the best interests of Europe, the United States and global economic growth, stability and security," he said (Alderman, 2016).

Britain has long been known as the financial capital of Europe and as an EU member, it has been able to protect this position by vetoing proposals to impose a single tax on the region's financial sector. London also won a victory at the European general court against a European Central Bank rule that would have moved the trading of securities priced in euros to countries that use the currency. Such a rule would have meant a huge loss of business for the banks that turned London into Europe's financial powerhouse. Nevertheless, with Brexit, the inability of Britain to participate in drafting the EU's rules may mean an end to its ability to coddle one of its biggest

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

industries - finance (Alderman, 2016). Thus, the stakes are huge and there is no room for error when deciding which path to choose.

Conclusion

The unavoidable reality which the UK faces as a result of Brexit, and its need to continue trading with the EU and the US, is that it must commit to data protection laws that are acceptable to it, the EU and US in order to avoid being subjected to trade barriers. How it does this must be decided as soon as possible and be in place by April of 2019. As such, it will have to accept one of the above discussed options.

An examination of each of the options in this paper leads to the conclusion that Britain likely adopt the General Data Protection Regulation (GDPR) or similar regulations.

Assuming the UK does implement the EU's GDPR, its primary goals must be to allow citizens to regain control of their personal data and cut red tape for international businesses by making rules uniform within the 28 (now 27) nation bloc (Batchelor, 2017).

On July 25, EU regulators approved the data transfer agreement and will not legally challenge it for at least a year, although activists or Europe's data protection authorities may still file complaints before then. But for now businesses on both sides of the Atlantic are relieved to have an agreement under which they can operate instead of the uncertainty and confusion which has existed since October of 2015. The July 25, 2015 WP29 statement is a positive step for the future of the Privacy Shield. So even though some concerns remain and legal challenges are likely. For the time being, the Privacy Shield remains a viable new mechanism for transferring data from the EU to the US. The regulation of data privacy, however, is an ongoing process that will never be subject to universal agreement.

Regardless of Britain's ultimate decision, meeting future data privacy regulations will come at a significant cost. Businesses with more than 30% of respondents polled expected their budgets to rise by more than 10% over the next two years as a result of the new data privacy regulations (Alderman, 2016). Estimates for the cost of businesses becoming GDPR compliant in Britain range from £320 million a year, and £2.1 billion over fourteen years. The EU itself predicts the cost to be £580m (Hawkins, 2015). Given this, any business with European transactions needs to pay attention to the viability of the privacy shield and how the UK decides to deal with its data transfer obligations post Brexit.

References

1. Alderman, L. (2016, July 13). After "Brexit", Britain could look to Norway as a model. *The New York Times*. Retrieved from https://www.nytimes.com/2016/07/14/business/international/after-brexit-britain-could-look-to-norway-as-a-model.html
2. American Civil Liberties Union. (2017, February 28). Joint letter to Commissioner Jourová Re: Privacy Shield. *Human Rights Watch*. Retrieved from https://www.hrw.org/news/2017/02/28/joint-letter-commissioner-jourova-re-privacy-shield
3. Ashford, W. (2015, December 8). New EU data protection laws to force global business strategy rethink. *ComputerWeekly*. Retrieved from http://www.computerweekly.com

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017

4. Baker, J. (2016, April 13). UK would need its own Privacy Shield deal with EU if it votes for Brexit. *ComputerWeekly*. Retrieved from http://www.computerweekly.com/news/450281222/UK-would-need-its-own-Privacy-Shield-deal-with-EU-if-it-votes-for-Brexit
5. Batchelor, T. (2017, January 24). One of the largest companies in the world has just threatened to pull some of its business from the UK. *Independent.* Retrieved from http://www.independent.co.uk/news/uk/home-news/brexit-latest-news-microsoft-major-companies-pull-business-from-uk-jobs-import-tariffs-eu-single-a7543641.html
6. Crabtree, J. (2016, July 7). Data flows post-Brexit: The next big headache for business? *CNBC*. Retrieved from http://www.cnbc.com/2016/07/07/data-flows-post-brexit-the-next-big-headache-for-business.html
7. Eriksson, A. (2016, July 7). Privacy Shield will not survive legal challenge, says Schrems. *Euobserver*. Retrieved from https://euobserver.com/digital/134322
8. European Commission Press Release. (2016). *EU Commission and United States agree on new framework for transatlantic data flows*. Retrieved from http://europa.eu/rapid/press-release_IP-16-216_en.htm
9. Hawkins, A. (2015, September 2). What will it cost to become EU data law compliant? *MyCustomer*. Retrieved from http://www.mycustomer.com/marketing/data/what-will-it-cost-to-become-eu-data-law-compliant
10. Kovacs, E. (2015, September 2). Industry reactions to Brexit: feedback Friday. *Security Week.* Retrieved from http://www.securityweek.com/industry-reactions-brexit-feedback-friday
11. Mason, R., Asthana, A., Rankin, J., & Boffey, D. (2017, March 31). UK may have to abide by EU laws during any Brexit transition phase. *The Guardian*. Retrieved from https://www.theguardian.com/politics/2017/mar/31/uk-may-have-to-abide-by-eu-laws-during-any-brexit-transition-phase
12. Massey, R. (2016). Brexit's impact on international data transfers. *Bloomberg Law Privacy and Data Security*. Retrieved from https://www.bna.com/brexits-impact-international-n57982076799/
13. McLellan, M., & Felz, J. (2016, June 28). Privacy shield developments and UK data transfers post-Brexit. *Data Privacy Monitor.* Retrieved from https://www.dataprivacymonitor.com/international-privacy-law/privacy-shield-developments-and-uk-data-transfers-post-brexit/
14. Meltzer, J. P. (2014). The importance of the Internet and transatlantic data flows for U.S. and EU trade and investment (No. 79). *Global Economy and Development*. Retrieved from https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf
15. Meyer, D. (2016, June 24). There may have been a breakthrough on the U.S.-EU privacy shield deal. *Fortune*. Retrieved from http://fortune.com/2016/06/24/privacy-shield-improvements/
16. Mullock, J., & Shooter, S. (2016). Brexit: Data protection and cyber security law implications. *Bird&Bird.* Retrieved from https://www.twobirds.com/en/news/articles/2016/uk/brexit-data-protection-and-cyber-security-law-implications
17. Nakashima, E. (2015, October 6). Top E.U. court strikes down major data-sharing pact between U.S. and Europe. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/eu-court-strikes-down-safe-harbor-data-transfer-deal-over-privacy-concerns/2015/10/06/2da2d9f6-6c2a-11e5-b31c-d80d62b53e28_story.html
18. Out-Law. (2016, July 5). Brexit: Minister admits the General Data Protection Regulation might not apply in the UK. *Out-Law.com.* Retrieved from https://www.out-law.com/en/articles/2016/july/brexit-minister-admits-the-general-data-protection-regulation-might-not-apply-in-the-uk/
19. Price, R. (2015, October 6). European Court of Justice rules on EU-US data transfer. *Business Insider*. Retrieved from http://www.businessinsider.com/ecj-safe-harbor-ruling-bots-expected-2015-10
20. Rodionova, Z. (2016, December 14). Brexit: 40% of US firms with British offices are considering relocating to the EU. *The Independent*. Retrieved from http://www.independent.co.uk/news/business/news/brexit-us-firms-trade-threat-london-eu-move-uk-relocate-move-report-a7473251.html
21. The High Court of Ireland. (October 6, 2015). *Schrems v Data Protection Commissioner (Case C-362/14).* Retrieved from http://cdt.org/files/2015/schrems.pdf
22. Weiss, M., & Archick, K. (2016). U.S.-EU data privacy: from safe harbor to privacy shield. *Congressional Research Service*. Retrieved from https://www.fas.org/sgp/crs/misc/R44257.pdf
23. Wilkerson, M., & Midgley, R. (2017, March 31). What is Article 50? The only explanation you need to read. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/0/what-is-article-50-the-only-explanation-you-need-to-read/

Submission date: 6 Jan. 2016; 1st Revision: 11 Oct. 2016; 2nd Revision: 27 Oct. 2016; 3rd Revision: 8 Nov. 2016; 4th Revision: 10 Nov. 2016; Acceptance: 21 Dec. 2017