Leaving the EU: the data protection implications of a 'Hard Brexit' for UK businesses with EU data flows and clients

Rachel A Masterton

A project submitted in partial fulfilment of the requirements of
Northumbria University for the Degree of
LLM Information Rights Law and Practice

Module - LA0331

Research undertaken in the School of Law

May 2018

16,983 words

DECLARATION

I declare that the work contained in this project is my own and that it has not been submitted for assessment in another programme at this or any other institution at postgraduate or undergraduate level. I also confirm that this work fully acknowledges the opinions, ideas and contributions from the work of others.

Signed:_____

Dated:_____

Table of Contents

Ethics Statement

The proposed research is based on secondary material or data already in the public domain (case law, journal articles, published surveys etc). It does not involve people in data collection through empirical research (eg. interviews or questionnaires). The ethical risk is low.

Chapter 1 - Introduction

On 9 January 2018 the European Commission's General Justice and Consumers Directorate ("the Commission") published a notice to stakeholders that dealt with the data protection implications of the UK's withdrawal from the European Union ("EU")[1]. It outlined the situation the UK could find itself on 30 March 2019, the date upon which the UK would leave the EU and no longer be subject to EU legislation; including that relating to the processing of personal data confirming that the UK would become a third country and that 'EU rules for transfer of personal data to third countries would apply'[2]. In under two pages, it outlined the situation that would exist in relation to data transfers; there would be methods to ensure existing data flows from EU Member States could continue but these would be an additional burden for UK organisations currently unnecessary.

Transfers of personal data to jurisdictions outside the EU are currently governed by provisions within Directive 95/46/EC[3] ("the DP Directive"). By the date of the UK's planned departure from the EU such transfers will come under the control of the Regulation 2016/679[4], otherwise known as the General Data Protection Regulation or GDPR. Less than a year after it comes into force across the EU, the GDPR will cease to have direct applicability to the UK but the Commission's notice[5] confirms that it will continue to have an impact on UK organisations that receive personal data from EU Member States. Furthermore, the UK is implementing its own national legislation that is intended to be equivalent to the GDPR. Therefore UK businesses will not be free from the reach of the EU in this area, despite the intention of Brexit.

Additionally, Article 3 of the GDPR makes it clear that organisations from outside the EU that process the personal data of data subjects who are within EU boundaries will

[1] --, 'Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection' (*European Commission* 09 January 2018) <http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245>
[2] ibid
[3] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data [1995] OJ L281
[4] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data [2016] OJ L119
[5] --, 'Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection' (*European Commission* 09 January 2018) <http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245>

be required to comply with its provisions. This extra-territoriality reinforces the EU's desire that its citizens benefit from the most up to date privacy protections and that businesses from within the EU should not be subject to more stringent controls than foreign organisations targeting its inhabitants.

This paper seeks to evaluate the additional obligations of the GDPR that will live on in the UK beyond its departure from the EU and what the UK Government could do to relieve some of those requirements. It will review case law surrounding data transfers and address the key messages from such judgments and their impact on processing going forward. It will draw on the musings of thought leaders in the arena of data protection and attempt to provide direction to the deliberations of organisations for which due regard to GDPR will remain a key part of governance come March 2019.

Chapter 2 - Background

2.1 Overview of GDPR

The GDPR[6] is an EU regulation governing the processing of personal data by organisations and the free movement of such data within the EU and, with appropriate safeguards, outside EU borders. Four years in the drafting, it replaces the DP Directive[7], creating, by virtue of its status as an EU Regulation, a harmonised approach to the protection of personal data across the EU and well beyond its geographical boundaries. The scope of the GDPR reflects the global digital environment organisations are now operating in and in which citizens' data is put to many, varied uses.

The GDPR was adopted in May 2016 and will be directly applicable across EU Member States from 25 May 2018, without the need for Member States to enact any enabling legislation. Whilst the GDPR has direct applicability there are several sections of the GDPR that have been left open for Member States to address with their own specific national legislation. In the UK, a Bill[8] is currently working its way through Parliament that will provide for, amongst other things, exemptions and derogations.

From 25 May 2018, organisations from outside the EU that target individuals within the EU with their goods or services or monitor their behaviour will also be required to comply with the new data protection framework[9], regardless of whatever legislative provision there is within their jurisdiction of operation that governs privacy and the processing of personal data.

The GDPR builds on the provisions within its predecessor, the DP Directive. It draws into its scope not only organisations operating outside the EU but organisations that

[6] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data [2016] OJ L119, p 0001-0081 ("GDPR")
[7] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data OJ L281 p 0035-0050
[8] Data Protection Bill [HL] 2017-19
[9] GDPR Article 3

operate as processors[10], whose actions were previously ungoverned by the DP Directive but instead contractually by data controllers. This greatly expands the number of organisations that are required to comply and as a result the regulatory burden falling on supervisory authorities, the arbiters of data protection compliance.

In addition to the broadening of scope, both organisationally and territorially, the GDPR strengthens existing data subject rights[11] and provides additional rights, such as the right to erasure[12] and the right of data portability[13]. The bolstered portfolio of rights that data subjects can exercise provides individuals with a greater degree of control over how their personal data will be used and requires organisations to improve data handling in response to this added awareness and the scrutiny by individuals that it brings with it.

Measures such as data protection by design and default[14] and the requirement for those undertaking riskier processing to designate a data protection officer[15] underpin the added principle of accountability[16] and the need for organisations to build compliance into all processing activities. Accountability in particular drives organisations to take stock of what they are doing with what is arguably their greatest business asset (aside from their employees) in a way that the DP Directive does not.

A key aspect of the DP Directive was the protection that personal data needed to be given when it left the shores of the EU. Lacking as it did the extra-territoriality provision of the GDPR, the data transfer requirements of the DP Directive gave it reach beyond the EU and required organisations not governed by the Directive or its associated Member State legislation to take measures to ensure transfers were adequately protected or risk no longer being attractive to EU organisations seeking services they provided.

[10] Specifically GDPR Article 28 but other aspects apply to processors as well as controllers
[11] GDPR Article 15 Right of access by the data subject
[12] GDPR Article 17
[13] GDPR Article 20
[14] GDPR Article 25
[15] GDPR Article 37
[16] GDPR Article 5(2)

The GDPR maintains the need for robust protections to be in place when personal data is transferred outside the EU and provides a number of measures to ensure that protection can be achieved. This further broadens the impact of GDPR, requiring as it does protections, to be in place for all personal data transfers outside the EU, not simply where there is an element of targeting or deliberate monitoring, as caveats the scope of extra-territoriality under Article 3.

A key part of the regulatory structure of the GDPR is the creation of the European Data Protection Board[17] ("the EDPB"), effectively the evolution of the existing Article 29 Working Party[18]. Comprising representatives from EU Member State supervisory authorities, the EDPB will resolve disputes between supervisory authorities and issue guidance on interpretation and implementation of the GDPR. It will hold a great deal of power over the manner in which personal data should be processed to comply with the requirements of the GDPR and promote cooperation and knowledge transfer worldwide. Its reach would seem to exceed traditional geographic boundaries, as with various aspects of the GDPR and have effect on far more jurisdictions than form its ranks. This means those external to the EU will be bound in one way or another by the EDPB's rulings without having any influence on its decisions.

2.2 'Brexit'

The EU's roots date back to the aftermath of the Second World War, when it was felt by various European countries that economic cooperation through trade would be a route to avoiding future conflict. The Schuman Declaration of 1950 proposed the creation of the European Coal and Steel Community, established in 1952, that as the name suggests, saw its member countries create a common market for coal and steel.

[17] GDPR Chapter VII: Section 3, Articles 68 - 76
[18] --, 'Article 29 Working Party' (*European Commission* no date) <http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358>

The Treaty of Rome in 1957 instigated the creation of the European Economic Community ("EEC") which came into being in 1958 and comprised initially Belgium, France, Italy, Luxembourg and West Germany. Its initial purpose was to create a customs union but that expanded in the early 1960s to encompass a common agricultural policy. Over the years, more countries applied to join the EEC, with the UK and Ireland becoming part of the EEC in 1973.

Recognising that member countries faced a number of policy issues that would benefit from a partnership approach, the remit of the EEC expanded to include, amongst other things health, the environment and justice. In 1993 this evolution was formally recognised by the signing of the Maastricht Treaty and the EEC changed its name to the European Union.

Through the EU, Member States' borders have been opened to other EU citizens and legislation is heavily influenced and directed from its headquarters in Brussels. Nineteen of the existing 28 EU Member States have rescinded their own currency and adopted the Euro, further strengthening trade links.

For a number of years, there has been concern expressed by some UK politicians and citizens that the EU has too much control over operations within the UK and that this was disadvantaging UK citizens and costing vast sums of money with little discernible benefit. On 23 June 2016 a referendum was held to resolve the conundrum of whether the UK should stay in or leave the EU[19]. More than 30 million people voted; a turnout of 71.8%. When the results were counted it was determined that 51.9% of those that voted wished to leave the EU, with 48.1% wanting to remain. This referendum and the subsequent withdrawal processes have been named 'Brexit'.

By virtue of the Treaty of Lisbon ("the Treaty"), signed by EU Member States in 2009, the referendum was not on its own enough to leave the EU. Article 50 of the Treaty outlines in five paragraphs how a country would part company with the EU. The UK

[19] Alex Hunt & Brian Wheeler, 'Brexit: All you need to know about the UK leaving the EU' (*BBC News* 30 January 2018) <www.bbc.co.uk/news/uk-politics-32810887>

invoked Article 50 on 29 March 2017 and so began a two year countdown to the UK's departure. The intervening period has seen numerous meetings to negotiate the UK's withdrawal and a number of different possible approaches being espoused by a variety of different sources.

A little over a year after Article 50 was triggered, there exists the possibility that a mutually agreeable resolution between the UK and the EU will not be forthcoming and the UK would experience what has been termed a 'hard' Brexit; a sudden ceasing of membership of the EU and the applicability of its associated policies, legislation and support. The UK Prime Minister has stated that it would be desirable to avoid such a 'cliff-edge'[20] but that a no deal is better than the wrong deal. What is clear is that the result from 23 June 2016 has implications for many aspects of life and governance within the UK and withdrawal is no simple task.

2.3 Impact of Brexit on GDPR

On 25 May 2018, when the GDPR becomes applicable across EU Members States, the UK will still be part of the EU and so UK organisations processing personal data will be required to comply with this new legislative framework. The Information Commissioner's Office ("the ICO") will be the UK's supervisory authority in accordance with Article 50 of the GDPR and representatives of that body will join the newly formed EDPB[21]. The EDPB replaces the existing Article 29 Working Party, convened under Article 29 of the DP Directive to discuss matters relating to the definition and application of that Directive, and is to be tasked with, amongst other things, monitoring and ensuring the correct application of the GDPR and resolving conflicts between supervisory authorities[22].

[20] ibid
[21] GDPR Article 68
[22] GDPR Article 70(1)

However, based on the provisions of Article 50 of the Treaty, on 29 March 2019 the UK will cease to be an EU Member State and will no longer be subject to the direct applicability of EU regulations, including the GDPR. At that point, if no provision is made to the contrary in the meantime, the UK will become a 'third country' in the eyes of the EU and subject to the restrictive provisions governing transfers of personal data outside the EU's geographical boundaries[23]. Data transfers that were acceptable the previous day will come under additional scrutiny, so much so that unless alternative measures are put in place those transfers will be prohibited[24]. This has the potential to hit businesses large and small across the UK and adversely impact on the attractiveness of organisations as trading partners, service providers and business locations in general.

Furthermore, the extra-territoriality nature of Article 3 of the GDPR will mean that many of those organisations reeling from the sudden change in data transfer status will, together with others monitoring the behaviour of individuals within the EU or targeting those individuals with goods or services, remain subject to the bulk of GDPR, regardless of whether the UK itself has data protection legislation of any kind. This could result in such organisations being burdened by some of the wide-reaching EU legislation some of the 51.9% of the public who voted for Brexit arguably wanted to be free from.

In addition, the ICO will no longer be entitled to sit on the EDPB and as such cease to have influence on the interpretation and application of the GDPR; a regulation the ICO had a hand in developing. It remains to be seen what impact the ICO's departure would have on the EDPB as a whole but what does seem definite is that as the UK's supervisory body they will need to have an eye on the EDPB's opinions and decisions without having a hand in their workings, further distancing the UK from the decision making that could ultimately impact upon it.

[23] GDPR Chapter V Articles 44 - 50
[24] GDPR Article 44

Chapter 3 - Options for Government : National Solutions

3.1 Membership of European Economic Area

The DP Directive stated goals that the EU had for the protection of personal data. However, by virtue of being an EU directive, it was not legally binding on Member States in the same way as the GDPR. Member States had to implement their own domestic legislation outlining how they were going to meet these goals. The Data Protection Act 1998 ("DPA") is that piece of legislation for the UK.

The Article 25 of the DP Directive explains that personal data should not be transferred to a third country (a country outside the EU) unless "the third country in question ensures an adequate level of protection"[25]. In the DPA, the eighth data protection principle is written in the spirit of that Article but with one key difference, replicated across the relevant EU Members States' domestic legislation. The eighth principle states that "personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data". The difference between that principle and Article 25[26] is the reference to the European Economic Area rather than the EU and it offers a possible option to the UK as they are negotiating their withdrawal from the EU.

The European Economic Area ("EEA") comprises the 28 EU Member States and three of the four European Free Trade Association ("EFTA"), namely Iceland, Liechtenstein and Norway. EFTA's mission is as "an intergovernmental organisation set up for the promotion of free trade and economic integration to the benefit of its four Member States – Iceland, Liechtenstein, Norway and Switzerland – and the benefit of their trading partners around the globe"[27]. Boosting the trading power of the four member countries since its inception in 1960 by the Stockholm Convention[28], EFTA has become

[25] DP Directive Article 25(1)
[26] DP Directive Article 25
[27] --, 'The European Free Trade Association' (*EFTA* no date) <www.efta.int/about-efta/european-free-trade-association>
[28] ibid

a key trading partner both for the EU and further afield. However, by being outside the EU, EFTA could suffer adversely from EU decisions, such as that relating to the protections necessary to transfer personal data beyond the EU borders.

In order to mitigate the risk of disadvantage, and to further enhance trading opportunities, three EFTA members, Iceland, Liechtenstein and Norway, joined with EU Member States to form the EEA, also known as the Internal Market. The EEA Agreement[29] came into force on 1 January 1994, guaranteeing equal rights and obligations for individuals and businesses within the Internal Market.

The EEA Agreement[30] set up and governs the EEA; the annexes to that document extend relevant EU Regulations and Directives to the three non-EU members. Annex XI - Electronic Communication, Audiovisual Services and Information Society[31] covers, amongst other things, the extension of various personal data related EU Directives and Regulations, most notably the DP Directive. As a result of this, references in the DP Directive to Member States are expanded to include the three additional countries; hence the reference in the DPA to transfers outside the EEA rather than simply outside the EU.

Relevant EU legislation is not automatically extended to the three ETFA members of the EEA. The EEA Joint Committee[32], a group comprising representatives of the EU and the three EFTA members, meets to agree the extension of new or amended EU legislation where such legislation covers the areas that form the remit of the EEA, namely the four freedoms[33] and the "flanking and horizontal"[34] policies. Should a Joint Committee Decision be forthcoming the relevant annex is amended, at which point the EU legislation is extended.

[29] --, 'Agreement on the European Economic Area' (*EFTA* 1 August 2016) <www.efta.int/ media/ documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the %20Agreement/EEAagreement.pdf>
[30] ibid
[31] --, 'Annex XI Electronic Communication, Audiovisual Services and Information Society' (*EFTA* 09 February 2018) <www.efta.int/media/documents/legal-texts/eea/the-eea-agreement/Annexes%20to%20the%20Agreement/annex11.pdf>
[32] --, EEA Joint Committee (*EFTA* no date) <www.efta.int/eea/eea-institutions/eea-joint-committee>
[33] The four freedoms are the free movement of goods, services, persons and capital
[34] Flanking and horizontal policies cover cooperation in important areas such as research and development, education, social policy, the environment, consumer protection, tourism and culture

Article 44 of the GDPR outlines the overarching principle for transfers of personal data; that personal data should not be transferred to third countries without adequate protections. The subsequent Articles deal with the different ways in which that protection can be established[35]. As with the DP Directive, the GDPR makes no particularly concession for the three EEA ETFA members.

Given that there is no automatic extension of new legislation and no reference to the EEA within the GDPR, the EEA Joint Committee needs to consider whether to extend the GDPR and whether any of the three EFTA members have any specific feelings around this.

At the time of writing (April 2018) a draft Joint Committee Decision was under consideration; the draft itself being dated 16 March 2018[36]. In light of the fact that to not extend the GDPR to the EEA would leave Iceland, Liechtenstein and Norway in the same position the UK may find itself after Brexit, it would be peculiar for it not to be and completely contrary to the aims of the EEA. For the purposes of this work, it will be assumed that when approaching data transfers from a practical perspective, the approach moves from being transfers outside the EU to transfers outside the EEA.

Therefore, UK membership of the EEA would maintain the free flow of personal data to jurisdictions within the EEA that the DPA currently provides and that it seems likely the GDPR will also enable. In addition, as it is to be assumed that to gain membership to the EEA the UK would need to join EFTA, the UK would be a party of what is the "ninth largest trader in the world in merchandise trade and the fifth largest … in services"[37], something that could be vital at a time when its trade links with the EU are severed.

However, membership of the EEA is not without its problems, particularly in light of the drivers behind Brexit and the stated positon of the negotiating team. Between 2014 and 2020 it is estimated that EEA EFTA countries will contribute EUR 3.22 billion to

[35] GDPR Articles 45 - 49
[36] --, '32016R0679 – Factsheet outlining incorporation of Regulation (EU) 2016/679 into EEA Agreement' (*EFTA* no date) <www.efta.int/eea-lex/32016R0679>
[37] --, 'The European Free Trade Association' (*EFTA* no date) <www.efta.int/about-efta/european-free-trade-association>

programmes in conjunction with the EU[38]. Given that a key driver for Brexit was a desire to stop sending vast sums of money to the EU, it would seem unlikely that the majority of UK citizens and some notable politicians would be agreeable to continuing to do so.

Furthermore, the UK has stated that it wishes to be part of the EDPB, the body replacing the current Article 29 Working Party. Whilst EEA EFTA members are currently subject to the decisions made by the Article 29 Working Party make, they do not have any particular input into its deliberations. This will continue under the GDPR. Therefore, the UK will still lose its voice at the decision making table.

However, a much more fundamental problem with this solution is that the Government has repeatedly stressed that it is not its intention to join EFTA. In its report entitled 'The United Kingdom's exit from and new partnership with the European Union'[39] chapter eight is dedicated to the stated desire to ensure free trade between the UK and Europe. Of the twelve chapters in this report this chapter is by far the longest, perhaps reflecting the importance that the Government puts on the need to maintain trading relations with the EU. The chapter opens with the statement that "The Government will prioritise securing the freest and most frictionless trade possible in goods and services between the UK and the EU". The very next sentence succinctly clarifies that this will not be through "membership of the Single Market".

This makes it clear that however helpful becoming a member of the EEA may be to preserving the existing free flow of personal data between the EU and the UK, a different solution will be necessary.

[38] --, EU Programmes with EEA EFTA Participation (*EFTA* no date) <www.efta.int/eea/eu-programmes>
[39] HM Government, 'The United Kingdom's exit from and new partnership with the European Union' (*gov.uk* 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/589189/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Print.pdf>

3.2 - Adequacy

In July 2017, the European Union Committee of the House of Lords published a report considering the data protection implications of Brexit[40]. This report was the culmination of Home Affairs Sub-Committee hearings at which evidence from a number of witnesses was heard and subsequently considered[41].

Discussion focused around data transfers and the various methods for ensuring what Matt Hancock MP described as "unhindered" and "uninterrupted"[42] data flows between the UK and EU once the UK was no longer a Member State. The European Union Committee of the House of Lords supported this objective[43] and following analysis of the discussion and evidence presented agreed with what it was said a "consensus amongst our witnesses"[44] that securing adequacy[45] from the Commission would be the most effective way of preserving data flows.

The importance of such a finding was highlighted by Elizabeth Denham, the UK Information Commissioner, who stated that whilst other countries manage to trade with the EU without an adequacy decision "the UK has been so heavily integrated in the EU that it is difficult to say that the UK can get by without an adequacy decision"[46].

Adequacy is not a new concept; it forms an integral part of the existing DP Directive[47] and enables third countries to apply to the Commission for recognition that their own data protection regime provides protection to personal data that is "essentially

[40] House of Lords, 'Brexit: the EU data protection package' (*parliament.uk* 18 July 2017) <https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf>
[41] ibid Appendix 2: List of witnesses
[42] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Rt Hon Matt Hancock MP, Minister of State for Digital and Culture' (*parliament.uk* meeting date 1 February 2017) <http://data.parliament.uk/writtenevidence/ committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/46835.html>
[43] House of Lords, 'Brexit: the EU data protection package' (*parliament.uk* 18 July 2017) <https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf> para 110
[44] ibid para 111
[45] GDPR Article 45
[46] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (*parliament.uk* meeting date 8 March 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48744.html>
[47] DP Directive Article 25(2)

equivalent"[48] to that found within the EU. The finding of an adequate level of protection enables personal data to be transferred to the relevant third country without any of the additional safeguards featured within the DP Directive thus reducing the complexity of such data flows.

Adequacy is assessed by the Commission, with input from the Article 29 Working Party, with consideration given to

> the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.[49]

Adequacy decisions can apply to transfers of all personal data or can be restricted to specific sectors or circumstances. Two of the existing twelve adequacy decisions are of the restricted type; the first of these applying only to transfers to commercial entities in Canada and the second in respect of transfers to specific, approved organisations within the United States, otherwise known as the EU-US Privacy Shield[50].

In a report published in January 2017[51], the Commission broke the twelve adequacy decisions into three groups, based on the perceived drivers for their adequacy application. The first group, comprising Switzerland, Andorra, Faeroe Islands, Guernsey, Jersey and the Isle of Man, was third countries "closely integrated with the European Union and its Member States"[52]; the second, made up of Argentina, Canada, Israel and the United States, was countries further afield but that had strong trading relationships with the EU and the third group, comprising New Zealand and Uruguay, was said to be countries "that have a pioneering role in developing data protection laws in their region"[53].

[48] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650 p.73
[49] DP Directive Article 25(2)
[50] --, 'Welcome to the Privacy Shield' (*Privacy Shield Framework* no date) <www.privacyshield.gov>
[51] --, 'Communication from the Commission to the European Parliament and the Council – Exchanging and protecting personal Data in a Globalised World' (*European Commission* 10 January 2017) <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN> pg 7
[52] ibid
[53] ibid

As an example, the Bailiwick of Guernsey ("Guernsey") took steps to secure an adequacy decision[54] under the DP Directive as soon as possible after the Data Protection (Bailiwick of Guernsey) Law, 2001 was enacted. Although it has its own parliament and legislature, Guernsey has close links with the UK by virtue of its status as a Crown Dependency and trading relationships with both the UK and the European mainland. This closeness of relationship was a key factor for Guernsey seeking an adequacy decision; in order to support its economy through good regulation at an equivalent level as the EU, to enable the free flow of personal data and to provide enhanced rights to data subjects.

Such is the benefit to its economy of having the adequacy decision, the States of Guernsey expressed its commitment to implementing new data protection legislation to meet the new standards set by the GDPR[55] within four months of the publication of the approved GDPR text. As a result, the Data Protection (Bailiwick of Guernsey) Law, 2017[56] was approved in November 2017[57], received Royal Assent from the UK Privy Council in March 2018[58] and will come into force on 25 May 2018[59], to tie in with GDPR becoming applicable.

A transfer on the basis of an adequacy decision[60] is the first of a number of measures that Member States can use to safeguard data transfers[61] under the GDPR. Existing adequacy decisions made under the DP Directive[62] will remain in force until they are amended, replaced or repealed[63]. This avoids, on 25 May 2018 when the GDPR becomes applicable, a sudden cessation of the data flows reliant on the twelve existing

[54] Commission Decision 2003/821/EC - on the adequate protection of personal data in Guernsey OJ L308, p 27-28
[55] --, 'General Data Protection Regulation' (*gov.gg* 16 September 2016) <www.gov.gg/gdprnews>
[56] Text can be viewed at www.guernseylegalresources.gg/CHttpHandler.ashx?id=112599&p=0
[57] --, 'Resolutions Billet XXII 29 November 2017' (*gov.gg* 29 November 2017) <www.gov.gg/CHttpHandler.ashx?id=111064&p=0>
[58] --, 'Data Protection Law Approved by UK Privy Council' (*gov.gg* 29 March 2017) <www.gov.gg/article/164773/Data-Protection-Law-Approved-by-UK-Privy-Council>
[59] --, 'The Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018' (*gov.gg* no date) <www.gov.gg/CHttpHandler.ashx?id=112468&p=0>
[60] GDPR Article 45
[61] GDPR Part V
[62] DP Directive Article 25(6)
[63] GDPR Article 45(9)

decisions and provides some leeway for any amendments to the legal framework in those third countries necessary to meet the higher GDPR standards.

As mentioned above, Article 45(9) of the GDPR states that existing adequacy decisions will remain in force until amended, replaced or repealed. This provision aligns with the review process that will be built into the adequacy process and demonstrates a more proactive approach to adequacy by the Commission going forward.

Article 45(3) of the GDPR makes it clear that adequacy decisions will be subject to periodic review "at least every four years"[64]. Such a provision does not exist in the DP Directive and indicates that adequacy decisions are not forever and that third countries that secure one will need to ensure standards do not slip over time. This reinforces the idea of the GDPR and the processes surrounding it having a global impact at a time when personal data and its processing has, in a significant way, become boundary blind.

Data transfers are far more common than they were in 1995 when the DP Directive was adopted and have, in some respects, become more opaque. In 1995, computer systems were located in the building in which the personal data upon them was used and transfers of personal data from one jurisdiction to another were conscious decisions. In the age of globalised systems, cloud computing and big data traditional boundaries have disappeared and even public authorities are contemplating moving data into 'the cloud', in some cases not fully appreciating where the cloud is tethered and what this means in relation to data protection provisions. This move away from contained processing and the need to design a data protection regime that does not lose pace with digital innovation has prompted a change in approach on a number of fronts, including that of data transfers. Implementing an adequacy decision without suitable governance in this environment is unthinkable, hence the review period[65].

[64] GDPR Article 45(3)
[65] ibid

Additionally, the Commission has made it clear that whilst a four year review period may exist, it is not sufficient for adequate third countries to sit back between reviews. The Commission will be implementing, in accordance with Article 45(4), an ongoing monitoring mechanism, pulling in and analysing information from a number of sources to keep a watching brief on the performance of those countries with adequacy decisions in order to act quickly if any problems should arise.

This triggering of an early review is confirmed by the Article 29 Working Party, who will continue to play a part in the granting of adequacy decisions when it becomes the EDPB on 25 May 2018. In its updated Adequacy Referential, it states "incidents or other information about or changes in the legal framework in the third country or international organization in question might trigger the need for a review ahead of schedule"[66]. The EDPB will be seeking to be fully involved in the review process and reiterated in the Adequacy Referential[67] the need for it to be furnished with all relevant documentation that would assist it fulfil its task in relation to adequacy decisions, as laid out in Article 70(1)(a)[68].

This monitoring process has already commenced in relation to the twelve existing adequacy decisions. Bruno Gencarelli, Head of the International Data Flows and Protection Unit at the Commission, stated at a conference of privacy professionals in September 2017[69] that contact had been made with representatives from the twelve adequate jurisdictions to clarify safeguards and intentions. This will form the basis of the ongoing monitoring, where Mr Gencarelli's team will scan material emerging from supervisory authorities, relevant government bodies, courts and the media to build a picture of the operation of the data protection regime in each given jurisdiction. This will flag issues that may need to be followed in a way that is not done under the DP Directive.

[66] Article 29 Working Party, 'Adequacy Referential (updated)' (*European Commission* 28 November 2017) <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48827>
[67] ibid
[68] GDPR Article 70(1)(a)
[69] Catherine Stupp, 'Commission conducting review of all foreign data transfer deals' (*Euractiv* 09 November 2017) <www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/>

Increased scrutiny of adequacy decision has not come about solely from the requirements of the GDPR. Prior to the publication of the final GDPR text, the adequacy process under the DP Directive was embroiled in a set of legal cases that ended up at the Court of Justice for the European Union ("CJEU") and put adequacy in the spotlight.

In 2000, Commission Decision 2000/520/EC[70] ruled that an arrangement whereby organisations in the United States could commit to handling personal data in a manner consistent with the DP Directive was adequate for the purposes of Article 25(2)[71] and would enable EU organisations to transfer personal data to these organisations and remain compliant with the transfer provisions of the DP Directive. This practice was known as "Safe Harbour".

The US did not at that time, and still does not, have any federal law governing the protection of personal data; instead each US State has their own legal framework. As a result, a traditional approach by the US to the Commission for adequacy was all but impossible. To enable privacy savvy organisations and those that recognised the value of free flowing data between the EU and themselves to make use of the adequacy provisions of the DP Directive the Safe Harbour scheme allowed organisations themselves to apply for and demonstrate a level of adequacy which, if achieved, would enable those data flows.

In May and June 2013, Edward Snowden, a former CIA contractor, leaked to the global media details of internet and phone surveillance by US intelligence agencies. This surveillance involved the tapping into the US-based servers of some of the largest, global internet firms. The surveillance program known as PRISM was alleged to have involved intelligence agencies breaking US privacy laws hundreds of times every year and the leaking of these details left Mr Snowden facing charges relating to the wilful

[70] Commission Decision 2000/520/EC - pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215, p 7 - 47

[71] DP Directive

communication of classified information as well as people around the world concerned for the safety of their personal data[72].

Following these revelations Maximillian Schrems made a request under Section 10(1)(a) of the Irish Data Protection Act 1998, as amended, ("the Irish DPA") for the Irish Data Protection Commissioner ("Irish DPC") to investigate whether Facebook had contravened the Irish DPA in relation to transfers of his personal data to the US. His case centred on the point that in his belief "the law and practice in force in that country [the US] did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities"[73].

The Irish DPC rejected Mr Schrems' complaint on the grounds that there was no evidence that his personal data had been accessed by US intelligence agencies[74]. Furthermore, the Irish DPC felt that the Safe Harbour agreement "stands as a formal decision of the EU Commission … under Article 25(6) of the Data Protection Directive 95/46/EC"[75] and as such provided an adequate level of protection. The Irish DPC concluded that "as Facebook-Ireland is registered under the Safe Harbour arrangement and as this provides for US law enforcement access, there is nothing for this Office to investigate."[76].

It transpired during later proceedings[77] that the Irish DPC had already approached Facebook Ireland with regards to the PRISM allegations prior to receiving Mr Schrems' complaint. In response to that approach Facebook Ireland confirmed that Facebook Limited, its US parent company, "did not provide access to US security agencies to subscriber data, save by means of targeted requests which were properly and lawfully

[72] --, 'Edward Snowden: Leaks that exposed US spy programme' (*BBC News* 17 January 2014) <www.bbc.co.uk/news/world-us-canada-23123964>
[73] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650
[74] Extract of a letter dated 25 July 2013 to Mr Schrems from the Irish DPC referred to in High Court judgement (*Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR, p31)
[75] Extract of a letter dated 26 July 2013 to Mr Schrems from the Irish DPC referred to in High Court judgement (*Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR, p30)
[76] ibid
[77] *Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR, p33

made"[78]. This assurance and an audit carried out by the Irish DPC provided him with satisfaction that appropriate mechanisms for dealing with requests from law enforcement and the like were in place.

Mr Schrems was not satisfied with this decision and referred the matter to the Irish High Court[79], raising again his concerns that his personal data had been subject to transfer and then interception by US intelligence agencies contrary to the protections offered under the Safe Harbour scheme.

Two important points came out of the hearing at the Irish High Court. The first related to the statement by the Irish DPC that Mr Schrems had no evidence of his personal data being compromised and so the complaint was "essentially hypothetical or speculative in nature"[80]. Mr Justice Hogan felt that the Snowden revelations demonstrated, "almost beyond peradventure"[81], surveillance of European citizens was being undertaken routinely by US security agencies and that in such circumstances "one may fairly question whether US law and practice in relation to data protection and State security provides for meaningful or effective judicial or legal control"[82].

Mr Justice Hogan therefore concluded that whilst Mr Schrems could not say whether his personal data had been accessed or was likely to be accessed, he was "entitled to object to a state of affairs"[83] that involved the transfer of his personal data to a jurisdiction where "only a limited protection against any interference"[84] was offered. This resulted in the case proceeding to the next step and serves as a useful precedent for other matters where a data subject may not be able to demonstrate they have been subject to potentially unlawful processing but where concerns can be underpinned by suitably reliable circumstantial evidence of apparent wrongdoing and will be a point

[78] ibid
[79] *Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR
[80] *Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR, p 41
[81] *Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR, p 42
[82] ibid
[83] *Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR, p45
[84] ibid

drawn upon in the future should other concerns about transfers and the risk to data subjects be expressed.

The major outcome from the Irish High Court was not in relation to the adequacy of the protections offered by Facebook Ireland when transferring personal data but was the lawfulness of the Safe Harbour scheme itself. Mr Justice Hogan found that by virtue of section 11(1) of the Irish DPA the Irish DPC "must determine the question of adequacy of protection in the third State 'in accordance' with a Community finding"[85] made by the Commission under Article 25 of the DP Directive. As such, it was judged that the Irish DPC could not investigate a complaint relating to a transfer made under a Commission decision of adequacy as the Irish DPC was bound by that decision.

Mr Justice Hogan stated that there was "perhaps, much to be said for the argument that the Safe Harbour Regime has been overtaken by events"[86] and cited the Snowdon leaks as an example of "gaping holes"[87] in US data protection practice. He recognised that the DP Directive and the Safe Harbour adequacy decision were enacted prior to the EU Charter of Fundamental Rights[88] ("the Charter") and the additional safeguards for personal data afforded by Article 7[89] and 8[90]. As a result, he referred the following questions to the CJEU :-

> Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in Commission Decision of 26 July 2000 (2000/520/EC) having regard to Article 7 and Article 8 of the Charter of Fundamental Rights of the European Union (2000/C 364/01), the provisions of Article 25(6) of Directive 95/46/EC notwithstanding? Or, alternatively, may the office holder conduct his or her

[85] *Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR, p 57
[86] *Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR, p 69
[87] ibid
[88] Charter of Fundamental Rights of the European Union 2012/C 326/02
[89] Charter of Fundamental Rights of the European Union 2012/C 326/02 – Article 7 Respect for private and family life
[90] Charter of Fundamental Rights of the European Union 2012/C 326/02 – Article 8 Protection of personal data

> own investigation of the matter in the light of factual developments in the meantime since that Commission Decision was first published?[91]

Taking the last question first, the CJEU considered whether a finding of adequacy by the Commission removed the ability for the supervisory authority in a Member State to act if a complaint was received concerning data transfers under that adequacy decision. In considering this matter the CJEU noted that the second sub paragraph of Article 25(6) of the DP Directive states that "Member States shall take measures necessary to comply with the Commission's decision"[92] and that as such a national supervisory authority could not "adopt measures contrary to that decision"[93] until such time as the decision itself was declared invalid by the Court. However, it went on to make the point that Article 28(4) of the DP Directive did not exempt or exclude the national supervisory authority from hearing claims from anyone concerned about the processing of their personal data that relate to an adequacy decision.

The key point is that once a national supervisory authority has investigated such a claim of non-compliance it cannot itself take any binding action "contrary to that decision"[94] if it feels the processing is not adhering to the decision or complying with the DP Directive. Instead the Member State must make provision for the national supervisory authority "to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling"[95], as was done in this case.

The CJEU moved from a decision as to the powers of the Irish DPC to consider the Safe Harbour scheme itself. Key to its deliberations was the self-certification nature of the scheme and whether, notwithstanding the different legal system in place in the US, the level of protection provided was "essentially equivalent to that guaranteed within the European Union"[96].

[91] *Schrems v Data Protection Commissioner* [2014] IEHC 310, 2013 765 JR, p 71
[92] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, p 52
[93] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, p 52
[94] ibid
[95] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, p 65
[96] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, p 74

The crux of Schrems' argument was the level of interference by US security services with the personal data held by Facebook and that it was incompatible with the Safe Harbour scheme. The CJEU highlighted that the Safe Harbour principles were "intended for use solely by US organisations receiving personal data from the European Union for the purpose of qualifying for the safe harbour and the presumption of 'adequacy' it creates"[97]. This restricted their impact to the self-certified entity only and US public authorities were not required to comply[98].

The CJEU also noted that the provisions of the Safe Harbour Commission Decision governed only the level of protection given in relation to the transfer itself, complying with Article 25(1)[99] of the DP Directive but not providing for the "protection of the private life and basic freedoms and rights of the individuals"[100]. This was due in great part to the Safe Harbour principles being limited to "the extent necessary to meet national security, public interest or law enforcement requirements"[101] and that where there was conflict between those principles and the US legal system, the organisations party to Safe Harbour must comply "with the law"[102] thus overriding its obligations under Safe Harbour.

It is reasonable that where there is a need to protect national security that relevant law enforcement and security bodies can request access to information they believe is of material relevance; to prevent this could have catastrophic consequences for the safety and wellbeing of citizens. However, sufficiently robust protections should be put in place to ensure that interference with an individual's rights and freedoms, including

[97] Commission Decision 2000/520/EC - pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215, p 7 – 47, Annex I
[98] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, p 82
[99] "The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."
[100] DP Directive Article 25(6)
[101] Commission Decision 2000/520/EC - pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215, p 7 – 47, Annex I
[102] Commission Decision 2000/520/EC - pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215, p 7 – 47, Annex IV Part B

their right to a private life and to the protection of their person data (Articles 7 and 8 of the Charter[103]) are justified, proportionate and targeted. This was confirmed by the CJEU in its judgment in the *Digital Rights Ireland and Others*[104] case in which it stated that "derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary"[105].

The CJEU found in the Schrems' case that the storage of personal data by the US security services could not be said to be 'strictly necessary' where it did not apply "any differentiation, limitation or exception"[106] to the data stored to ensure it met the objective or was capable of demonstrating and justifying the level of interference involved.

Commission Decision 2000/520[107] was declared invalid as a result, having immediate impact on EU-US transfer provision. It removed the mechanism by which a number of US companies had previously sought to demonstrate adequate protection for personal data and upon which EU organisations based their transfers for the purposes of Article 25(1)[108]. The judgment also hastened the implementation of the Privacy Shield[109], a revision of the Safe Harbour scheme that was already being worked on, in order to fill the void that was left.

Furthermore, the CJEU found that Article 3 of Commission Decision 2000/520/EC was incompatible with the DP Directive when read in conjunction with the Charter, limiting the extent to which national supervisory authorities could exercise their power in relation to transfers to adequate jurisdictions[110]. Whilst this had no material impact on the Safe Harbour regime itself, given it was declared invalid in its entirety, the judgment with regards to national supervisory authorities' power led to an alteration of

[103] Charter of Fundamental Rights of the European Union 2012/C 326/02
[104] *C-293/12 and C-594/12 Digital Rights Ireland and Others* [2014] EU:C:2014:238
[105] ibid para 52
[106] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650, para 93
[107] Commission Decision 2000/520/EC - pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215, p 7 - 47
[108] DP Directive Article 25(1)
[109] Commission Decision 2016/1250 – pursuant to Directive 95/46/EU of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207, p 1 - 112
[110] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650

all remaining adequacy decisions[111], clarifying that if a national supervisory authority has sufficient concern regarding the protection of personal data subject of one of these decisions they could suspend the transfer, temporarily or indefinitely and engage in legal proceedings.

However, the judgment also has wider and longer lasting repercussions. It has added to the scrutiny that existing and new adequacy decisions may be under. Prior to this judgment, it would seem that national supervisory authorities felt unable to challenge a Commission decision of adequacy. This case makes it clear that if a data subject raises legitimate concerns that when investigated call into question the validity of an adequacy decision, the national supervisory authority should feel able to put a stop to such transfers and refer the matter to the national courts for onwards referral to the CJEU.

More importantly for the UK and any potential application for adequacy is the impact over-reach by a jurisdiction's national security services may have on the initial granting and onwards retention of an adequacy decision. The Snowdon revelations of mid 2013[112] not only referred to surveillance activities of the US intelligence agencies; reference was made to similar activities by the UK security services and the broad nature of the methods employed to gain information for national security purposes.

In December 2016, the CJEU ruled in a case involving, amongst other parties, the UK's Secretary of State for the Home Department that dealt with the retention of communications data for national security purposes[113]. Questions relating to what constituted a legitimate and proportionate interference with the privacy rights of

[111] Commission Decision 2016/2295 – amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the adequate protection of personal data by certain countries, pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council OJ L344 p 83 - 91

[112] --, 'Edward Snowden: Leaks that exposed US spy programme' (*BBC News* 17 January 2014) <www.bbc.co.uk/news/world-us-canada-23123964>

[113] *C-203/15 and C-698/15 Tele2 Sverige AB and Others* [2016] ECLI:EU:C:2016:970

individuals were referred to the CJEU by the UK Court of Appeal[114] following an appeal by the Secretary of State as a result of the hearing at the High Court[115].

Directive 2002/58/EC ("the E-Privacy Directive") provides for the protection and privacy of data processed in the provision of electronic communications; electronic communications comprising telecommunications (phone and facsimile), email and SMS. It lays down various measures that must be complied with to ensure a suitable level of protection is provided to individuals when using these forms of communication. Article 15(1) of the E-Privacy Directive provides for Member States to restrict by way of derogation some aspects of those protections

> when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.[116]

The CJEU was asked to rule on whether the Data Retention and Investigatory Powers Act 2014 ("DRIPA") was compatible with EU legislation, in particular the Charter[117] and Article 15(1) of the E-Privacy Direct as amended[118]. Section 1 of DRIPA provided the Secretary of State with the power to request telecommunications providers retain communications data for the purposes outlined in section 22 of the Regulation of Investigatory Powers Act 2000 ("RIPA"). The purposes include national security[119], prevention and/or detection of crime or disorder[120], protecting the economic wellbeing of the UK[121] and tax collection and assessment[122].

[114] R (on the application of Davis MP and others) v Secretary of State for the Home Department [2015] EWCA Civ 1185, [2015] AllER (D) 196
[115] *R (on the application of Davis MP and others) v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin)
[116] Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337 p 11 - 36
[117] The Charter - Articles 7, 8 and 52
[118] Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337 p 11 - 36
[119] RIPA s 22(2)(a)
[120] RIPA s 22(2)(b)
[121] RIPA s 22(2)(c)
[122] RIPA s 22(2)f)

Three individuals had originally expressed concern at the breadth of this power and had sought judicial review, drawing parallels between the legislation and the ruling in the *Digital Rights Ireland* [123]case that had already been heard at the CJEU. In the case of DRIPA, the CJEU felt that the circumstances in which communications data could be retained exceeded those specifically listed in Article 15(1) of the E-Privacy Directive.

Furthermore, the CJEU felt that the access to retained communications data would be a serious interference with the rights afforded to individuals by the Charter and as such, in relation to the "prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime is capable of justifying such access to the retained data"[124].

Following on from that, the CJEU considered that even with the clarification that access should be in circumstances related to the fighting of serious crime, an appropriate prior review of the request for access should be carried out "by a court or by an independent administrative body"[125] and granted only where deemed necessary, save for circumstances of "validly established urgency"[126]. Individuals whose data was subject to such a request should also be advised of the access, when to do so would not prejudice the purpose for which access was granted, enabling the individual to exercise their right to legal remedy[127].

Since that ruling DRIPA has expired and been replaced by the Investigatory Powers Act 2016 but similar issues with regards its incompatibility with EU legislation have recently been ruled upon. Following a hearing earlier this year, a judgment published by the Divisional Court[128] found that section 4 of the Investigatory Powers Act 2016 was "incompatible with fundamental rights in EU law"[129] as a result of access to

[123] C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] EU:C:2014:238
[124] C-203/15 and C-698/15 *Tele2 Sverige AB and Others* [2016] ECLI:EU:C:2016:970 para 115
[125] C-203/15 and C-698/15 *Tele2 Sverige AB and Others* [2016] ECLI:EU:C:2016:970 para 120
[126] ibid
[127] C-203/15 and C-698/15 *Tele2 Sverige AB and Others* [2016] ECLI:EU:C:2016:970 para 121
[128] *R (on the application of the national council for Civil Liberties (Liberty)) v Secretary of State for the Home Department and another* [2018] EWHC 975 (Admin)
[129] ibid para 186

communications data not being restricted to that necessary to combat serious crime and was not subject to the prior review the CJEU should be put in place. The conclusion of the judgment was that the necessary amendments must be made to the legislation by 1 November 2018[130].

The problem with the UK's surveillance powers was raised at the Home Affairs Sub-Committee meetings that led to the House of Lords report on Brexit and data protection[131]. The UK ICO, Elizabeth Denham stated at the hearing on 8 March 2017 that "From recent CJEU judgments, it seems likely that the UK's surveillance and data retention regime would be at[sic] risk for a positive adequacy finding"[132] and suggested that it was an area that required Government attention if the UK wanted to seek an adequacy decision.

This reiterated similar evidence given at an earlier hearing by Ruth Boardman. She explained that whilst part of the EU the national security concerns "cannot be used as a reason to prevent a free flow of data within the UK"[133]; the Commission being unable to make a judgement on the adequacy of protections for Member States. She went on to explain that in much the same way as Safe Harbour, concerns about national security over-reach "could be used as a reason for arguing that the UK ought not to be adequate"[134].

Following the recent deadline imposed upon the Government for the revision of the problematic areas of the Investigatory Powers Act 2016[135], it is entirely possible that the problem that may well jeopardise adequacy would not exist by the time of the UK's

[130] ibid
[131] House of Lords, 'Brexit: the EU data protection package' (*parliament.uk* 18 July 2017) <https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf>
[132] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (*parliament.uk* meeting date 8 March 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48744.html>
[133] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Antony Walker, Deputy CEO, techUK; Ruth Boardman, Co-Head, International Data Protection Practice, Bird and Bird' (*parliament.uk* meeting date 1 February 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/49297.html>
[134] ibid
[135] *R (on the application of the national council for Civil Liberties (Liberty)) v Secretary of State for the Home Department and another* [2018] EWHC 975 (Admin)

departure from the EU. However, it is an area of sufficient risk to warrant remedial action being taken now not only to amend that piece of legislation but to review others for possible incompatibility and address any such areas with alacrity.

There remains a further potential problem with regards to the application for an adequacy decision. The GDPR provides for the Commission to assess whether a third country or an international organisation provides an adequate level of protection to personal data[136]. It therefore suggests that the Commission could not consider a request from the UK until it is a third country.

However, in a speech by the Prime Minister in March 2018, Rt Hon Theresa May MP emphasised that the free flow of data was "critical for both sides in any modern trading relationship"[137] indicating that a delay the adequacy process would be detrimental. Following this speech, former UK Information Commissioner Richard Thomas stated that in his opinion "some sort of 'deemed' adequacy recognition should be included"[138] in the agreement reached governing the UK's departure from the EU. This possible way forward acknowledges the "unique positon"[139] the UK will find itself in, as alluded to by Baroness Williams of Telford her appearance before the House of Lords' European Union Committee, having already spent almost a year under the GDPR regime by the earliest possible exit date of March 2019.

3.3 Bespoke Arrangement

In the Prime Minister's speech of early March 2018[140], reference was made to the desire for what has been described by some as an "adequacy plus"[141] solution for data

[136] GDPR Article 45
[137] --, 'PM speech on our future economic partnership with the European Union' (*GOV.UK* 2 March 2018) <www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union>
[138] Rezzan Huseyin, 'UK PM's Ambitious' data protection plan not unreasonable, say experts' (2018) PDP 18 4 (1) (2)
[139] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Baroness Williams of Trafford, Minister of States, Home Office' (*parliament.uk* meeting date 26 April 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/ evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/69266.html>
[140] --, 'PM speech on our future economic partnership with the European Union' (*GOV.UK* 2 March 2018) <www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union>
[141] Rezzan Huseyin, 'UK PM's Ambitious' data protection plan not unreasonable, say experts' (2018) PDP 18 4 (1) (2)

transfers. The Rt Hon Theresa May stated that more than a traditional adequacy decision would be sought in recognition of trading links between the UK and the EU. She explained that the UK would be seeking "an appropriate ongoing role for the UK's Information Commissioner's Office"[142] that would enable UK organisations to be encompassed in the "one-stop-shop"[143] regime, designed to harmonise data protection regulation across the EU and enable greater cooperation between supervisory authorities.

The "one-stop-shop" mechanism enables organisations established across a number of Member States to interact primarily with the supervisory authority in the jurisdiction in which they have their main establishment. This means either where their headquarters is based, or the location of their data protection expertise. The mechanism is designed to streamline the administrative burden of operating in more than one Member State and provides for the supervisory authority in the jurisdiction of a company's main establishment to take the lead on compliance matters, including the investigation of complaints. In the Article 29 Working Party's guidance on determining the lead supervisory authority[144], it makes it clear that this is a mechanism open only to those organisations with their main establishment in an EU Member State. Organisations whose main establishment is outside the EU would be required to interact with the supervisory authority in each country of operation, potentially through their representative[145].

Therefore, when the UK leaves the EU its organisations that operate cross-border would be unable to take advantage of the "one-stop-shop" and would be presented with an increased regulatory burden. This could add to the inevitable discussions around boardroom tables as to whether being established in the UK is something multi-national companies would view as an untenable situation, when taking into account current uncertainty in a number of areas, not just data protection.

[142] --, 'PM speech on our future economic partnership with the European Union' (*GOV.UK* 2 March 2018) <www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union>
[143] GDPR Article 60 and Recital 127
[144] Article 29 Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority' (*European Commission* 5 April 2017) <http://ec.europa.eu/newsroom/document.cfm?doc_id=44102>
[145] GDPR Article 27

As such, and as recognised by both the Prime Minister[146] and the UK Information Commissioner[147], a continued role for the ICO both as part of the "one-stop-shop" and the EDPB would be advantageous to UK business and enable the ICO to continue to apply what is frequently seen as a pragmatic voice[148] to EU data protection discussions. Eduardo Ustaran, Partner at Hogan Lovells and well-known to UK data protection practitioners, stated that "the adequacy-plus aim is certainly bold and ambitious"[149] but went on to remark that the UK is seen as a safe place for personal data and that "if it retains the EU's legal framework irrespective of Brexit – which the UK is clearly doing – why should the outcome change?"[150].

Whatever the merits of the arguments for adequacy-plus, whether it becomes part of the final withdrawal arrangements will not be known for some time. However, in January 2018 the Commission endorsed proposals first articulated in January 2017 that as "the protection of personal data is a fundamental right in the EU, it cannot be subject to negotiations in the context of EU trade agreements"[151]. This perhaps suggests that the EU would be unwilling to include data protection in the Brexit negotiations recognising instead that the "preferred avenue for the EU are 'adequacy decisions'"[152] and that there is limited room for manoeuvre within the GDPR.

[146] --, 'PM speech on our future economic partnership with the European Union' (*GOV.UK* 2 March 2018) <www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union>
[147] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (*parliament.uk* meeting date 8 March 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48744.html>
[148] House of Lords, 'Select Committee on the European Union, Home affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Antony Walker, Deputy CEO, techUK; Ruth Boardman, Co-Head, International Data Protection Practice, Bird and Bird' (*parliament.uk* meeting date 1 February 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/49297.html>
[149] Rezzan Huseyin, 'UK PM's Ambitious' data protection plan not unreasonable, say experts' (2018) PDP 18 4 (1) (2)
[150] ibid
[151] --, 'College Meeting : European Commission endorses provisions for data flows and data protection in EU trade agreements' (*European Commission* 31 January 2018) <http://europa.eu/rapid/press-release_MEX-18-546_en.htm>
[152] ibid

Chapter 4 - Options for Data Controllers & Processors : Organisational Solutions

4.1 Standard Data Protection Clauses

The DP Directive enabled the Commission to approve standard clauses that could be used by controllers within the EEA when transferring personal data to a third country. These were known variously as 'standard contractual clauses' and 'model clauses'. By using these clauses, obligations were placed on both the sending and receiving organisation to ensure the rights and freedoms of the data subjects were protected.

Two sets of clauses were approved for transfers from a controller within the EEA to a controller out with of the EEA; the first in June 2001[153] and the second in 2004[154]. These were further authorised by the UK ICO in accordance with the DPA[155]. Either set of clauses can be used and organisations can choose which one fits their requirements best; the key difference being the former provides the data subject with a direct right of action against both parties with the exporting and importing organisations being jointly and severally liable, whereas the latter set restricts the data subject to only being able to enforce their rights against the party responsible for any breach.

Clauses also exist for use between an EEA based controller and a processor based outside the EEA. Whilst two sets have been approved by the Commission and the UK ICO, only the newest set, approved by the Commission in February 2010[156], can now be used for new transfer arrangements. The currently approved set of clauses, in a similar way to the newest controller to controller clauses, allow, as the UK ICO says "liability to follow fault"[157] enabling the data subject to take action against the organisation that has caused the breach.

[153] Commission Decision 2001/497/EC –on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC OJ L181 p 19 - 31
[154] Commission Decision 2004/915/EC – amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries OJ L385 p 74 - 84
[155] --, 'Model Contract Clauses – International transfers of personal data' (*ICO* no date) <https://ico.org.uk/media/for-organisations/documents/1571/model_contract_clauses_international_transfers_of_personal_data.pdf
[156] Commission Decision 2010/87/EU – on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council OJ L39 p 5 - 18
[157] --, 'Model Contract Clauses – International transfers of personal data' (*ICO* no date) <https://ico.org.uk/media/for-organisations/documents/1571/model_contract_clauses_international_transfers_of_personal_data.pdf>

A key point to bear in mind with the existing clauses is that an organisation can only benefit from the Commission's decision regarding the adequate safeguards provided if the clauses are not altered in any way. They can feature as part of a stand-alone contract dealing specifically with the data transfer part of a relationship or can be added to a more comprehensive document that covers all necessary aspects of the contractual arrangements. However, if added to another contract it should be done wholesale with no changes to the wording, "even if the meaning or effect of the changed clause remain[s] unaltered"[158].

Article 46 of the GDPR provides for transfers subject to appropriate safeguards. Contractual clauses feature as two of these appropriate safeguards, renamed as standard data protection clauses. These can be adopted by the Commission[159] or by a supervisory authority then approved by the Commission[160] and both serve as an appropriate safeguard for data transfers "that enforceable data subject rights and effective legal remedies for data subjects are available"[161].

It would seem that the existing clauses will continue to be applicable post 25 May 2018 subject to any appending to contracts information necessary to comply with other aspects of the GDPR – such as joint controller[162] or processor responsibilities[163]. Indeed, in the Notice to Stakeholders[164] released by the Commission in January 2018 that covered effectively what options existed for transfers post Brexit if no deals were forthcoming, reference was made to the three sets of model clauses outlined above. It is suggested that these will remain valid until amended or rescinded by the Commission.

[158] --, 'Model Contract Clauses – International transfers of personal data' (*ICO* no date) <https://ico.org.uk/media/for-organisations/documents/1571/model_contract_clauses_international_transfers_of_personal_data.pdf
[159] GDPR Article 46(2)(c)
[160] GDPR Article 46(2)(d)
[161] GDPR Article 46(1)
[162] GDPR Article 26
[163] GDPR Articles 28 and 29
[164] --, 'Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection' (*European Commission* 09 January 2018) <http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245>

However, the fallout from the Schrems' challenge to Safe Harbour[165] has potential implications for the three sets of clauses currently available. Following the decision by the CJEU that the Safe Harbour transfer mechanism was invalid Facebook reverted to relying on the standard contractual clauses as an appropriate safeguard for data transfers. The Irish DPC was concerned that this did not provide the level of safeguards appropriate and lacked elements of the legal redress that were necessary for the rights and freedoms of the data subject to be respected, especially in connection with the Charter[166].

The matter was considered the Irish High Court and the judgment of Ms Justice Costello was that the concerns were well-founded in particular with relation to those data subjects whose personal data "is wrongly interfered with by the intelligence services of the United States"[167] once transferred there. As such, she referred the "issue of the validity of the SCC [standard contractual clauses] decisions to the CJEU for a preliminary ruling"[168] and sought submissions with regards to the questions to be posed.

This matter is yet to be considered by the CJEU but in light of the Safe Harbour case and the changes made to existing adequacy decisions it is entirely possible, particularly when personal data is transferred to the US using these clauses, that they will be deemed not to provide the necessary safeguards. It is too early to determine exactly what implications this will have for the UK post-Brexit but it is an area on which to keep a close watch. Whilst the use of standard data protection clauses will remain part of the GDPR whether they will be in the current form is less clear and organisations may wish to consider whether they want to dedicate time to putting such arrangements in place now in preparation for Brexit or whether time would be better spent considering the other options available, at least until the CJEU have provided their preliminary judgment.

[165] *C-362/14 Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650
[166] --, 'Explanatory Memos on the litigation Concerning Standard Contractual Clauses – Explanatory Memo dated 28 September 2016' (*Irish Data Protection Commissioner* 26 September 2016) <https://dataprotection.ie/viewdoc.asp?DocID=1598&ad=1>
[167] *Data Protection Commissioner v Facebook Ireland Limited and another* [2017] IEHC 545 p. 339
[168] *Data Protection Commissioner v Facebook Ireland Limited and another* [2017] IEHC 545 p. 340

4.2 Binding Corporate Rules

Binding Corporate Rules ("BCRs") enable global companies to transfer personal data within the same corporate group beyond EU borders. Devised by the Article 29 Working Party as a mechanism to demonstrate sufficient safeguards in accordance with Article 26(2) of the DP Directive, BCRs first came into existence in June 2003[169]. Prior to this, data transfers within and across multi-national companies were subject to contracts featuring the standard contractual clauses[170] and many such documents were needed to capture all relevant data flows, creating a system that was burdensome.

BCRs mean that a framework can be constructed that operates for a variety of intra-group transfers and as a requirement a proper understanding of the way personal data flows around the organisation and the use to which it is put is necessary. This means that the process of developing BCRs adds a level of governance to the processing that other transfer mechanisms may not. Furthermore, there is an obligation to monitor compliance and the efforts made to train staff across the company as well as providing the lead authority with an annual update to ensure the BCRs remain appropriate. As a result, the accountability now required by the GDPR[171] has arguably been demonstrated by organisations making use of BCRs for a number of years.

Each set of BCRs, by virtue of Article 26(2)[172], is assessed by one of the EU national supervisory authorities, determined in much the same way as the GDPR "lead supervisory authority"[173] concept. For a number of years, if that authority was satisfied that the safeguards contained within the BCRs were adequate they were circulated to other supervisory authorities for comment and approval[174]. The organisation

[169] Article 29 Working Party, 'Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers" (*European Commission* 3 June 2003) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf>
[170] See section 4.1 above
[171] GDPR Article 5(2)
[172] DP Directive Article 26(2)
[173] GDPR Article 56
[174] --, 'Binding corporate rules' (*ICO* no date) <https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/>

submitting the BCRs for approval dealt solely with the lead authority, with that authority coordinating and facilitating the process, a pre-cursor to the GDPR "one-stop-shop" arrangements in effect.

Since April 2011, 19 EU Members States have adopted a mutual recognition process for BCRs, meaning that if one country's supervisory authority approves a set of BCRs, the other 18 "have confidence in their decision and accept their findings without further scrutiny or comment"[175]. The UK is one of those 19 and has acted as the lead authority for approximately 25% of all BCRs currently in place[176].

BCRs have been specifically written into the GDPR as a means of demonstrating the safeguards necessary for international data transfers[177]. In addition, the Article 29 Working Party has confirmed that, subject to additional measures being addressed to bring the compliance measures up to the GDPR's level, existing BCRs can continue to be relied upon[178]. This has provided a degree of assurance to organisations already using these arrangements that they do not have to start again.

As mentioned above, around a quarter of the BCRs approved to date have been done so by the UK ICO. With Brexit on the horizon and uncertainty about the ICO's status once no longer an EU supervisory authority, the Deputy Information Commissioner - Operations, James Dipple-Johnstone, published a blog in November 2017 to provide some clarity. Here it made it clear that companies subject to BCRs previously approved by the ICO "will need to ensure they (and all their data processing) are GDPR compliant)"[179] and that they could inform the ICO of those changes as part of their annual update.

[175] --, 'Binding corporate rules' (*ICO* no date) <https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/>
[176] Dipple-Johnstone J, 'Changes to Binding Corporate Rules applications to the ICO' (*ICO* 20 November 2017) <https://iconewsblog.org.uk/2017/11/20/changes-to-binding-corporate-rules-applications-to-the-ico/>
[177] GDPR Article 46(b) & Article 47
[178] Article 29 Working Party, 'Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules' (*European Commission* 29 November 2017) <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798> section 1.2 Amendments of already adopted BCRs
[179] Dipple-Johnstone J, 'Changes to Binding Corporate Rules applications to the ICO' (*ICO* 20 November 2017) <https://iconewsblog.org.uk/2017/11/20/changes-to-binding-corporate-rules-applications-to-the-ico/>

Furthermore and perhaps more importantly, Mr Dipple-Johnstone stated "that no BCR authorisations will be cancelled because of Brexit"[180] and that the ICO would seek to continue to work with EU supervisory authorities to ensure that "the ICO's leading expertise in BCR is continually available to the international controller and processor community"[181]. The latter statement is perhaps a lofty one, given the lack of clarity around the role the ICO will play on the European stage post-Brexit. However, it does provide necessary assurances that those organisations currently using BCRs would not be plunged into chaos come March 2019.

BCRs certainly have merit as an intra-group transfer mechanism for post-Brexit transfers particularly where data flows outside the UK and EU are already in existence and as such there remains around a year in which to prepare the necessary submission and await the approval. Sometimes referred to as the 'gold star' of data transfers the accountability and governance surrounding BCRs sits well with the requirements of GDPR. However, the limiting factor is the restricting of such measures to within one corporate structure, leaving any external data transfers needing an alternative, appropriate mechanism.

4.3 Codes of Conduct

Codes of conduct are not new in the field of data protection. The DP Directive makes reference to them as measures "to contribute to the proper implementation"[182] of Member States' legislation, hence the inclusion of codes of practice in the DPA[183]. Therefore the inclusion of codes of conduct in the GDPR[184] is no surprise.

What is new is the specific list of circumstances where codes of conduct are deemed particularly appropriate[185]. One of these areas is "the transfer of personal data to third

[180] ibid
[181] ibid
[182] DP Directive Article 27(1)
[183] DPA 1998 s53(3) & (4)
[184] GDPR Article 40
[185] GDPR Article 40(2)(a)-(j)

countries"[186]. Article 46(2)(e) elaborates on this point and states that when "binding and enforceable commitments"[187] are given by the controller or processor in the third country that the safeguards in such a code of conduct are to be adhered to it can be used as an appropriate safeguard making the transfer lawful.

In some respects, such a commitment may offer a better level of protection than the standard data protection clauses, as the organisation will be subject to monitoring[188]. This provides a level of assurance around the processing safeguards that the standard data protection clauses do not and puts codes of conduct on a similar footing to BCRs. In the same way as BCRs, they should effect change in the manner in which personal data is processed in order to maintain compliance and the safeguards and benefits that they bestow rather than the organisation simply relying on legal remedies.

A monitoring body will have the power to "take appropriate action"[189] should it find an organisation not complying with the code of conduct as it should. Such action can include the suspension or exclusion of the organisation from the code[190], therefore removing the safeguards relied upon for the transfer. This does not remove the ability for the supervisory authority to also review the processing and deal with it accordingly. And whilst proper adherence to a code of conduct can be a mitigating factor when a supervisory authority is considering an administrative fine, "non-compliance could be an aggravating one"[191] and lead to an increased fine.

A further element of robustness is the fact that not only will the organisation making use of the code of conduct be subject to monitoring, but the monitoring body itself will be accredited and subjected to scrutiny by the relevant supervisory authority[192]. The accreditation as a monitoring body can be revoked by a supervisory authority if the conditions for accreditation[193] are not met and, in extreme circumstances, a fine can be

[186] GDPR Article 40(j)
[187] GDPR Article 46(2)(e)
[188] GDPR Article 41
[189] GDPR Article 41(4)
[190] ibid
[191] Rita Heimes, 'Top 10 operational impacts of the GDPR: Part 9 – Codes of conduct and certifications' (*IAPP* 24 February 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/>
[192] GDPR Article 41
[193] GDPR Article 41(2)

imposed on a monitoring body of up to EUR 10,000,000 or 2% of global annual turnover[194].

Furthermore, unlike standard data protection clauses, a code of conduct can be drafted to specifically deal with a particular industry sector and so tailored to the processing they cover and the safeguards that work best in relation to that processing. Codes of conduct can be drafted by industry bodies and other third party organisations as well as supervisory authorities and an appropriate degree of consultation with interested parties is necessary before being approved. This makes the result robust and specific and something in which data subjects should be able to put their faith.

There are two main drawbacks at this time with this option. The first is that there are no existing codes of conduct dealing with transfers and the exit of the UK from the EU moves ever closer. The second is that once the UK is no longer part of the EU the ICO may not be considered to be a competent authority for such codes of conduct. In such a circumstance it would be necessary for the drafting, approval and accreditation to be driven from within one of the remaining 27 EU Member States. Whether such measures are as important for the relevant supervisory authorities as they are for the organisations in the UK remains to be seen. However, as the GDPR requires the drafting of codes of conduct to be encouraged, by the time such a document is necessary there may well be something appropriate in existence.

4.4 Certification

Certifications are a new concept in relation to data protection although as Rita Heimes explains "for years, certification marks and seals have served as useful signals for consumers interested in engaging with commercial entities that adhere to certain desirable principles"[195]. In an era in which the value of data to both the consumer and

[194] GDPR Article 83(4)
[195] Rita Heimes, 'Top 10 operational impacts of the GDPR: Part 9 – Codes of conduct and certifications' (*IAPP* 24 February 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/>

the organisation has increased and data protection reform has placed an emphasis on data ethics, it is appropriate that controllers and processors are given an opportunity to flag their good practice to attract privacy savvy individuals to use their goods or services.

Underpinned by binding and enforceable commitments, a certification can be used as an appropriate safeguard for the purposes of data transfer[196] and so could have value for a UK based organisation following Brexit. An organisation seeking a certification will be required to provide the awarding body with "all information and access to its processing activities which are necessary to conduct the certification process" following which a full assessment of the processing will be conducted. A certification will be valid for a maximum period of three years at which point it could be renewed if appropriate standards are maintained.

As with codes of conduct, the supervisory authority will be able to accredit certification bodies although "the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012"[197] will also be able to accredit certification bodies, as long as they are cognisant of any additional requirements the relevant supervisory authority may have.

Earlier this year the Article 29 Working Party released for consultation draft guidelines on the accreditation of certification bodies. The aim of these guidelines is to "help Member States, supervisory authorities and national accreditation bodies establish a consistent, harmonised baseline for the accreditation of certification bodies that issue certification in accordance with the GDPR"[198]. It is encouraging that these guidelines should soon be adopted by the Article 29 Working Party as it should mean that by the time UK organisations need to use such measures proper processes are in place. It also

[196] GDPR Article 46(2)(f)
[197] GDPR Article 43(1)(b)
[198] Article 29 Working Party, 'Draft Guidelines on the accreditation of certification bodies under regulation (EU) 2016/679' (*European Commission* 6 February 2018) <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877>

reveals the importance that the GDPR places on certification in general as a means of demonstrating compliance and best practice.

These guidelines also serve to explain the importance of the accreditation process that will underpin the certification mechanism. It states that the "particular value and purpose of accreditation lies in the fact that it provides an authorative statement of the competence of certification bodies that allows the generation of trust in the certification mechanism"[199]. Therefore, in much the same way as employees may be attracted to an employer displaying the Investors in People[200] certification, consumers in the future may seek out service providers that have been awarded an equivalent data protection certification and best practice becomes a business driver.

4.5 Derogations

Despite the variety of different methods for ensuring an adequate level of protection for personal data transferred outside the EU, provision is made within the GDPR for those occasions when adequate protection cannot be attained but when there is still a pressing need to transfer personal data. These derogations are outlined in Article 49[201] and are broadly similar to the derogations currently provided for data transfers under the DPA[202].

It is important to remember, when transferring personal data using any of the derogations, that the derogations themselves provide no protection for the data transferred. They are designed to provide a fall back position for those occasions when there is a need to transfer the data even though the level of protection does not meet that expected within the EU or afforded by other transfer mechanisms. The ICO's international transfers guidance caveats the use of derogations under the DPA, stating that "in interpreting these provisions, the derogations should be narrowly

[199] ibid
[200] --, 'What is Investors in People?' (*Investors in People* no date) <www.investorsinpeople.com/what-investors-people>
[201] GDPR Article 49
[202] DPA Schedule 4

construed"[203]. This guidance should form part of the decision making process when considering use of derogations under GDPR.

Furthermore, whilst the use of a derogation may enable a controller or processor to transfer personal data when other protection measures are not available, the derogation does not remove the need for the controller or processor to comply with the rest of the GDPR. Controllers must still comply with the principles found in Article 5; the first of which is to identify which of the lawful processing conditions is being relied upon for the transfer and to ensure that the data subject has the information required under Article 13[204] or 14[205], including that relating to the transfer itself. There can be very few circumstances where personal data should be transferred outside the EU without the data subject having been made aware that the transfer will happen.

An assessment of each derogation is given below to provide an indication as to when each may be used and any specific considerations necessary.

- Article 49(1)(a) Explicit consent

  This derogation makes it clear that the consent must be explicit and that the data subject must be fully informed of the risks of the transfer in light of no adequate protection mechanism being in place. Article 7[206] already raises the standard of consent to make it specific to a defined circumstance, unambiguous, freely given and capable of being withdrawn or withheld. This means that consent would not be deemed valid if it was presumed or vague consent with the related information being buried in the small print of a terms and conditions document.

  However, this derogation requires consent to be 'explicit'. Some may suggest that the redefined consent already strays into the realms of explicit consent given its

[203] --, 'The eighth data protection principle and international data transfers' (*ICO* 30 June 2017) <https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf>
[204] "Information to be provided where personal data are collected from the data subject"
[205] "Information to be provided where personal data have not been obtained from the data subject"
[206] "Conditions for consent"

affirmative and specific nature. The Article 29 Working Party, in their guidance specifically related to consent[207], clarifies that explicit consent remains a higher level of consent that that outlined in Article 7[208] and suggests that "An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement". The guidance goes on to state that a written statement would not be the only way to confirm this and that electronic versions of this mechanism or a two stage verification process could also be acceptable.

The higher standards to be adopted when using this derogation extends to the information to be given to the data subject in order to inform their decision. The data subject's attention must be drawn to the specific risks that their personal data may be exposed to as a result of the transfer and the lack of protection the derogation offers[209]. This is in addition to the usual transparency information that should be provided to data subjects as part of Articles 13[210] and 14[211].

What is clear is that the extra high level of consent required for this derogation to be used reinforces the concept that derogations should be used as something of a last resort and that it is inappropriate, not to mention lacking the necessary robustness and stability, to make the consent derogation part of standard business practice.

- Article 49(1)(b) Performance of a contract with data subject & Article 49(1)(c) Conclusion or performance of a contract in the interest of the data subject

  At first glance these two derogations appear to be somewhat wide and may appeal to organisations looking to overcome the problem of not being able to make use of

[207] Article 29 Working Party, 'Guidelines on Consent under regulation 2016/679' (*European Commission* 28 November 2017) <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849>
[208] GDPR Article 7
[209] Article 49(1)(a)
[210] "Information to be provided where personal data are collected from the data subject"
[211] "Information to be provided where personal data have not been obtained from the data subject"

the other transfer mechanisms. However, it is not simply a case of putting whatever transfers an organisation wishes to carry out in contract form.

The key word for both contract derogations is 'necessary'; the transfer has to be necessary for the performance or conclusion of the contract or as part of pre-contractual measures taken at the data subject's request. In this context necessary means that the transfer is an integral and vital part of the contract. The relevant Article 29 Working Party guidance[212] and the ICO's guidance[213] both cite holiday bookings as being occasions when a transfer would be necessary in connection with a contract.

Conversely, transfers that are as a result of the manner in which an organisation has chosen to conduct or structure its business may not always be deemed necessary. An example given by the ICO relates to the paying of employees and states that whilst paying an employee is a necessary part of an employment contract, if the payroll function is centralised outside the EU for the convenience of the employer "it would be difficult to show that the centralisation … is objectively necessary for the performance of the data subject's employment contract and could not be carried out elsewhere".

In addition, recital 111 provides additional context restricting the derogations' use to situation "where the transfer is occasional and necessary in relation to a contract". In the payroll example given above very nature of payroll means that the processing is highly unlikely to be only occasional and instead subject to a very regular pattern. Therefore, even if a convincing argument can be put together to justify the necessity of the transfer in the payroll example the derogation would still fail to be a lawful basis for the transfer on the grounds of regularity.

[212] Article 29 Working Party, 'Guidelines on Article 49 of Regulation 2016/679' (*European Commission* 6 February 2018) <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846>
[213] --, 'The eighth data protection principle and international data transfers' (*ICO* 30 June 2017) <https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf>

Furthermore, where the data subject is not the instigator of the contract with the contract being between an organisation and a third party, for the contract derogations to be applicable the transfer needs to be occasional[214], necessary, and in the interests of the data subject[215], again heavily restricting the situations in which this can be relied upon and narrowing the apparently broad applicability that a quick perusal of these derogations may falsely suggest.

Whilst there is no doubt that the contract derogations can be useful and have validity in certain circumstances, organisations need to carefully review their use to ensure the derogations are not applied incorrectly. The oft heard explanation of 'that's the way it's always been' is not likely to stand the scrutiny that transfers using the contract derogations may attract and organisations need to be very clear when making use of them that they have addressed each aspect and documented their deliberations appropriately.

- Article 49(1)(d) Important reasons of public interest

Use of this derogation would seem to hinge on two key points. Firstly, the identification of the public interest and the important reasons underpinning it; recognising what FOI practitioners have learnt, that public interest is not the same as what is interesting to the public. Secondly, as with the previous derogation, the transfer must be necessary for those important reasons.

An important note in the ICO transfers guidance[216] is that the public interest to be considered is that of the Member State rather than the third country to which the data is transferred. Therefore, however persuasive the third country organisation is in putting together a justification of why it is in their public interest, this derogation

[214] GDPR Recital 111
[215] GDPR Article 49(1)(c)
[216] --, 'The eighth data protection principle and international data transfers' (*ICO* 30 June 2017) <https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf>

cannot be utilised if a robust justification in the public interest of the Member State is not in existence.

Recital 58 of the DP Directive lists examples of where transfers using this derogation may be justified; transfers "between tax or customs administrations in different countries"[217] or "between services competent for social security matters"[218].

- Article 49(1)(e) Establishment, exercise or defence of legal claims

This derogation, relating to transfers for the establishment, exercise or defence of legal claims, again requires the organisation to justify why such transfer is necessary rather than simply something that would be of assistance.

The ICO also draws attention to "the need to balance the legal rights at the centre of the advice or action with the data subject's rights in relation to their personal data"[219]. The need to perform such an assessment is increased when using this derogation as there may well be a corresponding exemption that if engaged would exempt the organisation from the need to comply with various data subject rights.

Certainly this situation exists at present within the DPA. The non-disclosure exemption at section 35 refers to "establishing, exercising and defending legal rights"[220] and can be utilised to exempt the organisation from the following requirements :-

- Provision of fair processing information relating to the disclosure[221]

[217] DP Directive Recital 58
[218] ibid
[219] --, 'The eighth data protection principle and international data transfers' (*ICO* 30 June 2017) <https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf>
[220] DPA 1998 section 35
[221] DPA 1998 Schedule 1 first data protection principle

- Further use of the personal data to be compatible with the purpose or purposes for which it was originally processed[222]
- Personal data to be adequate, relevant and not excessive[223]
- Personal data to be accurate and up to date[224]
- Personal data to be held for no longer than necessary[225]
- The right to object to processing that causes damage or distress[226]
- The right to rectification, blocking, erasure and destruction[227]

Combining the exemption at section 35[228] with the derogation relating to legal rights[229] can realistically result in an individual's personal data being used in another jurisdiction, with inadequate protections, without them knowing, with no requirement for the data to be used for the purposes they would be expecting, to be accurate, concise or destroyed when no longer needed. Furthermore, should they find out about the data's transfer and use they may be unable to exercise several of the rights that could assist them in regaining an element of control.

As such, it is important that a proper, thorough assessment of the merits of the transfer are balanced against the impact on the data subject and the risk to their data that the transfer may pose. A high threshold should be set to ensure that any interference with a data subject's rights and protections is justifiable, particularly where any exemption from such rights and protections may be utilised in conjunction with the derogation.

- Article 49(1)(f) Protect vital interests

[222] DPA 1998 Schedule 1 second data protection principle
[223] DPA 1998 Schedule 1 third data protection principle
[224] DPA 1998 Schedule 1 fourth data protection principle
[225] DPA 1998 Schedule 1 fifth data protection principle
[226] DPA 1998 section 10
[227] DPA 1998 section 14
[228] DPA 1998
[229] DPA 1998 Schedule 4 derogation 5

A similarly high level of definition of vital interests is needed when considering this derogation as is necessary when using the similarly worded lawful processing condition. Vital interests is defined by the ICO as being "matters of life and death"[230] and its use relies on the fact that the data subject is physically or legally incapable of giving consent for the transfer. Therefore this derogation would cover the transfer of medical details to a third country in order to treat a patient that was unresponsive.

However, the Article 29 Working Party explains that there is a requirement for immediacy or an "essential diagnosis"[231]. Use of this derogation for medical research purposes with a longer period of time until the benefits of the processing will be felt would not be lawful. Neither is it where the data subject is capable of giving consent, when explicit consent in accordance with Article 40(1)(a) would be a more appropriate derogation to utilise.

- Article 49(1)(g) Public register

This derogation enables the transfer of information that forms part of a public register that is "open to consultation either by the public in general or by any person who can demonstrate a legitimate interest"[232]. The electoral register is an example of such a register and can be viewed by the public, usually in a public library[233].

The caveat to this derogation is that the transfer should not involve the whole register or "entire categories of the personal data contained in the register"[234]. In essence this means that a person can request access to records within a public

[230] --, 'The eighth data protection principle and international data transfers' (*ICO* 30 June 2017) <https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf>
[231] Article 29 Working Party, 'Guidelines on Article 49 of Regulation 2016/679' (*European Commission* 6 February 2018) <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846>
[232] GDPR Article 49(1)(g)
[233] --, 'The electoral register and the open register' (*gov.uk* no date) <www.gov.uk/electoral-register/view-electoral-register>
[234] GDPR Article 49(2)

register that are of particular interest but cannot, as one would expect, end up with the entire register, just as a member of the public cannot take the electoral register home with them but can view records they require.

The GDPR has also made provision for transfers to be made where "necessary for the purposes of compelling legitimate interests pursued by the controller"[235] and where it cannot be based on any of the protection measures contained within Article 45[236], Article 46[237], including binding corporate rules[238] or any of the derogations discussed above. Heavy caveats apply to such a transfer however, as one would expect of an absolute last resort. Transfers making use of this provision should not be repetitive in nature, should only involve the data of a limited number of data subjects and with suitable safeguards put in place following an assessment of "all the circumstances of the transfer"[239] in order to mitigate the risk. In addition, the controller must notify the relevant supervisory authority of the transfer.

Whilst this notifying of the supervisory authority seems to be simply that at this stage, letting the supervisory authority know of the transfer rather than asking for prior authorisation, the supervisory authority has the power "to order the suspension of data flows to a recipient in a third country"[240]. Therefore, it should be expected that a register of such transfers will be kept and where any patterns emerge that suggest the transfers are repetitive or include more than a limited number of data subjects the supervisory authority will look further into the transfers and, if concerned, could order the suspension of such processing. As such, this is quite definitely an option to be used sparingly and when all other options have been thoroughly exhausted. It is not in any way a solution upon which to build an organisation's transfer activities.

A final point of note in relation to the transfer provisions in Article 49 concerns their use by public authorities, or rather, in keeping with the tightening of approach with

[235] GDPR Article 49(1) second sub-paragraph
[236] Transfers on the basis of an adequacy decision
[237] Transfers subject to appropriate safeguards
[238] GDPR Article 47
[239] GDPR Article 49(1) second sub-paragraph
[240] GDPR 82(j)

regards to public authorities shown in other areas of the GDPR[241], how the use of some of these provisions is restricted in relation to public authorities. Article 49(3) states that the explicit consent[242], performance of a contract[243] and conclusion of a contract[244] conditions together with the compelling legitimate interests condition[245] are not to be used by a public authority in the exercise of their public functions.

Whilst it could be argued that public authorities tend to operate within their own jurisdiction's boundaries by virtue of their role, where data does need to be transferred to other locations it is vitally important that proper, well considered processes are put in place based on the mechanisms that offer appropriate levels of protection. Only in very limited circumstances should citizens' personal data be transferred without such protection, recognising that in the majority of cases citizens do not have the option to be selective as to which public authorities collect and process their personal data in the way they can with private sector organisations.

4.6 Extraterritoriality and Representatives

Article 27 of the GDPR opens with the statement that "Where Article 3(3) applies, the controller or the processors shall designate in writing a representative in the Union"[246]. Article 3(3) relates to the extra-territorial nature of the GDPR and the fact that the GDPR is applicable to any organisation outside the EU boundaries that targets data subjects in the EU with goods or services, or offers thereof, or monitors the behaviour of data subjects inside the EU.

Once the UK ceases to be an EU Member State it is imperative that trade with the EU remains. Discussion within this paper so far relates to the ways in which organisations

[241] For example, inability for public authorities to rely on the legitimate interest condition (Article 6(1) second sub-paragraph) and the need for all public authorities to designate a data protection officer (Article 37(1)(a))
[242] GDPR Article 49(1)(a)
[243] GDPR Article 49(1)(b)
[244] GDPR Article 49(1)(c)
[245] GDPR Article 49(1) second sub-paragraph
[246] GDPR Article 27(1)

within the EU can be assured that personal data transferred to the UK for which they are accountable will be adequately protected making the transfer lawful in accordance with Article 45. However, the extra-territoriality provision within Article 3 extends the protections of the GDPR to EU citizens who decide to deal directly with organisations outside the EU and the representative requirement forms part of the demonstration of accountability and the commitment of organisations to the GDPR.

In essence, this means that on the date that the UK leaves the EU, regardless of what data protection regime is in place within the UK, organisations offering goods or service within the EU's geographic boundaries will have to comply with the GDPR. For organisations that have put in place measures to comply with the GDPR and will still trade within the EU, there may be little difference in day to day operations. For organisations that had perhaps hoped that withdrawal from the EU would mean they could attempt to ignore the GDPR, Article 3 may not be the news they were hoping for.

Whatever the outlook of an organisation, upon withdrawal from the EU, if their activities fall within those outlined in Article 3(3) they may need to appoint a representative to comply with Article 27, an article they could safely ignore while the UK was an EU Member State.

Article 27(2) states that the requirement to appoint a representative does not apply where the processing is occasional, does not include large scale processing of special category data and "is unlikely to result in a risk to the rights and freedoms natural persons, taking into account the nature, context, scope and purposes of the processing"[247]. The representative requirement also does not apply to public authorities[248]. Terms such as 'occasional' and 'large scale processing' are not defined within Article 27 or at any point in the GDPR. However, the Article 29 Working Party has released guidance that whilst not focused on Article 27 does provide their thoughts

[247] GDPR Article 27(2)(a)
[248] GDPR Article 27(2)(b)

on both "occasional"[249] and "large scale"[250] and until more clarity is available may be the best place to start.

Those organisations, both controllers and processors, that do not benefit from Article 27(2), will be required to employ the services of a representative. Article 27 states that a representative should be established in one of the EU Member States in which the organisation's data subjects are based, that the representative will be mandated to be addressed in addition to or instead of the organisation by supervisory authorities and data subjects and that the arrangement will be without prejudice to legal actions against the organisation themselves.

An internet search does not provide a great deal of further information about Article 27 and how the representative will work. A screenshot of the first page of results can be found at Appendix 1. The first ten results provides three links to Article 27; two results are commentary, noting that there is little further advice in existence; and two are people seeking further advice. The final three links relate to representative services being offered to organisations that will be captured by Article 27 from 25 May 2018.

Given that the Commission, the Article 29 Working Party and EU Member State supervisory authorities are focused on ensuring the relevant frameworks and guidance are in place for EU Member States in time for 25 May 2018, it is perhaps unsurprising that guidance on an element of the GDPR that only impacts organisations outside the EU has not yet been provided. There are perhaps other areas of the GDPR that these bodies can concentrate on that would have a greater impact in the short time left than this matter.

However, it seems incompatible with the idea of adequacy that an adequacy decision, awarded where the Commission decides a jurisdiction's legislative framework is

[249] Article 29 Working Party, 'Guidelines on Article 49 of Regulation 2016/679' (*European Commission* 6 February 2018) <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846>
[250] Article 29 Working Party, 'Guidelines on Data Protection Officers ('DPOs') (*European* Commission 13 December 2016) <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048>

essentially equivalent to that of the EU[251], does not seemingly remove the need for the representative, despite an adequacy decision demonstrating the jurisdiction's commitment and cooperation.

It is to be hoped that by the time the UK exits the EU, further guidance or case law as to how Article 27 is to be interpreted and indeed how it works in practice will be available to assist those organisations that may be required to secure the services of a representative. But in the meantime, it may prove useful for organisations to think about how they would be able to address compliance with this area as failure to comply could conceivably result in a fine of up to €10,000,000 or 2% of global turnover for preceding year[252] particularly if combined with other areas of non-compliance.

[251] GDPR Article 45
[252] GDPR Article 83(4)(a)

Chapter 5 - Conclusion

After a lengthy period of drafting, persuasion, lobbying and redrafting, the final text for the GDPR was published on 25 May 2016, with it due to become applicable across EU Member States two years later. After the backwards and forwards around what would and would not make the final version, the direction for all Member States was set, with implications for those outside the geographical boundary as well as within, and a period of preparation and implementation period.

For the UK, this fixed end point was firm for less than a month before the Brexit referendum, with a small majority but with great repercussions, decided that the UK would be leaving the EU. Data protection practitioners, organisations and the ICO found themselves grappling with uncertainty – not only would they need to prepare for the GDPR but they would need to be ready to respond to the outcome of the Brexit process and whatever that meant for data protection.

At the time of writing this conclusion, the GDPR countdown clock stood at twenty days with the UK's withdrawal from the EU scheduled to occur a little over ten months after that. Yet despite the uncertainty of what the post-Brexit data protection world may look like, a recent survey showed that UK organisations were more prepared than EU counterparts for 25 May 2018, with 62% of UK respondents saying they would be compliant by that date[253], compared with an EU figure of 46%.

Furthermore, whilst the UK has yet to enact national legislation to deal with those areas of GDPR that have been left for Member States to determine individually, the Data Protection Bill [HL] 2017–19 was due to both move to the Report stage and receive its third reading in the House of Commons on 09 May 2018[254]. This was with a view to enactment by 25 May 2018. Whilst not leaving much time for unforeseen

[253] Peter (Spiceworks), 'Most will miss GDPR deadline: UK most prepared, US and rest of EU lag behind' (*spiceworks* 02 May 2018) <https://community.spiceworks.com/blog/3023-most-will-miss-gdpr-deadline-uk-most-prepared-us-and-rest-of-eu-lag-behind>
[254] --, 'Bill stages – Data Protection Bill [HL] 2017–19 (*www.parliament.uk* no date) <https://services.parliament.uk/Bills/2017-19/dataprotection/stages.html >

problems, only four of the 28 EU Member States had similar legislation in place[255], putting the UK in a reasonable state by comparison.

The way in which the UK has embraced GDPR and the progress towards compliance shows that organisations are aware it is coming and its implications. Whether this is purely driven through fear of the mammoth fines or an understanding of the business enabler GDPR could be if approached correctly is difficult to say. However, it does show a nation that, despite what the Brexit vote may have indicated, has taken this piece of EU legislation on board and are working to find ways to deal with it.

This paper evaluated the various ways in which data transfers could be conducted in accordance with the GDPR between the 27 remaining EU Member States and the UK and the other implications of its extra-territorial reach. There is no doubt that personal data will continue to flow from the EU to jurisdictions not captured by the GDPR's direct applicability; in the globalised digital world we now live it would be impossible for it not to and for the EU to continue as a major trading body.

As for the UK, statements emanating from Government show how important trade will be post-Brexit. The role that data protection has to play in relation to ongoing trade is demonstrated by it featuring in key Government messages as we move towards March 2019. Whether it be the inclusion of the Data Protection Bill in the Queen's Speech[256] following the 2017 general election or the Prime Minister's 'adequacy-plus' plan from early March 2018[257], data protection and maintaining a means of sharing personal data with organisation inside the EU has been firmly placed on the agenda for Brexit negotiations.

This is encouraging as by far the best way to ensure the necessary free flows of personal data would be for the UK to be granted adequacy under Article 45[258]. Whilst

[255] Meyer D, 'Most member states won't be ready for GDPR' (*iapp* 24 April 2018) <https://iapp.org/news/a/most-member-states-wont-be-ready-for-gdpr/>
[256] --, 'Queen's Speech: New data protection law' (*BBC News* 21 June 2017) <www.bbc.co.uk/news/technology-40353424>
[257] --, 'PM speech on our future economic partnership with the European Union' (*GOV.UK* 2 March 2018) <www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union>
[258] GDPR Article 45

this approach will require effort from the Government, legislators and the ICO, it removes the burden of resolving the transfer problem from the shoulders of UK organisations and the EU counterparts with which they wish to deal.

Achieving adequacy demonstrates that the rights of the individual are built in at all levels of the legal framework and that personal data will be respected and safeguarded in a manner essentially equivalent to the GDPR. Adequacy provides a robust set of protections, under increased levels of scrutiny built into the GDPR and arising from legal challenge, that will apply to UK citizens' data as well as that transferred from the EU. Whilst such protections would also come from the UK joining the EEA, as has been discussed, there seems little appetite for that from those leading the negotiations as it ties the UK down not only in relation to data protection but in many other areas too.

It is true that the UK will be in a different positon than any other jurisdiction that has applied for adequacy previously. GDPR will have had direct effect on the UK for the preceding ten months so in theory demonstrating the necessary standards should be straightforward. However, three issues remain that should be addressed. They are the potential for a gap between leaving the EU and achieving adequacy; the role of the ICO on the European stage; and the perceived overreach of UK surveillance activities.

As discussed, the GDPR allows for third countries to be granted adequacy by the Commission and until it leaves the EU the UK will not be a third country. The assessment of a jurisdiction's adequacy is a lengthy process and if not commenced until after Brexit would leave the UK facing the 'cliff-edge'[259] alluded to by the UK Information Commissioner in the Home Affairs Sub- Committee meetings of early 2017. However, in reality this is an administrative problem and an assessment could be built into whatever transition arrangements arise from the Brexit negotiations.

[259] House of Lords, 'Select Committee on the European Union, Home Affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (*parliament.uk* meeting date 8 March 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48744.html>

Alternatively, given the UK's unique positon of already having lived under GDPR, the granting of a 'deemed'[260] adequacy may be possible with the necessary, future reviews built around it by the Commission. This would work in much the same way as the 'rolling over' of existing adequacy decisions, which were granted under the less robust DP Directive but will remain in place until a review is undertaken, either according to a schedule devised by the Commission or in response to concerns raised at the level of protection provided. The timing issue is, therefore, in no way insurmountable.

The role of the ICO going forward is not so straightforward. Whilst the ICO plays a crucial role on the Article 29 Working Party now, providing what has been described as a pragmatic voice of reason, by strict interpretation of the GDPR it will have no such right to remain on the EDPB once the UK has parted company with the EU, or to be part of the 'one-stop-shop'. The Government has expressed its desire for a resolution to be found to enable the ICO to remain part of these functions but it is in no way clear that the Commission would be prepared to enable that.

The EEA countries, who arguably have closer links with the Commission than any third country, are not likely to be included in the EDPB in any capacity other than observer and are not considered part of the 'one-stop-shop' at this time. To admit the UK's supervisory authority to these two constructs would be inequitable with the status of the EEA countries and could lead to demands for their inclusion also. Furthermore, there are twelve other adequacy decisions in existence and to admit the ICO may lead to requests from the other adequate jurisdictions, potentially increasing the membership of the EDPB in total by around two thirds.

At this point, reference should be made again to the endorsement by the Commission of proposals dating from January 2017 that state that data protection and the safeguards it provided were too important to be included in negotiations and stressing that adequacy was the "preferred avenue"[261]. This may be the clearest indication of

[260] Rezzan Huseyin, 'UK PM's Ambitious' data protection plan not unreasonable, say experts' (2018) PDP 18 4 (1) (2)
[261] --, 'College Meeting : European Commission endorses provisions for data flows and data protection in EU trade agreements' (*European Commission* 31 January 2018) <http://europa.eu/rapid/press-release_MEX-18-546_en.htm>

the thoughts of the Commission on the suggestion to continue to treat the ICO as any other Member State supervisory authority and, as such, the ICO needs to continue its efforts to develop its status on the international stage as well as its measures to interact with its former EU compatriots.

The third issue, relating to the extent to which UK legislation enables law enforcement bodies to access the personal data of individuals in a manner deemed incompatible with the Charter, was one also raised at the Home Affairs Sub-Committee meetings and had the potential to be a sticking point for any adequacy application[262]. The invalidation of the Safe Harbour mechanism[263] and the verdict in the DRIPA[264] case demonstrates how critically the CJEU views surveillance overreach.

Had this conclusion been drafted two weeks earlier than it was, it would have ended by stressing how important it would be for the Government to take appropriate action to address the lasting issues from the DRIPA[265] case. It cannot be over-emphasised how detrimental UK legislation's perceived incompatibility with the Charter would be to an adequacy assessment. However, the High Court judgment published on 27 April 2018[266] has imposed a November deadline for remedial action to remove this incompatibility from the latest iteration of DRIPA[267]. Whether this is sufficient to remove surveillance as a concern remains to be seen and may only really be understood at the time of assessment. The tackling of the incompatibility does, however, serve to strengthen the protections and safeguards for personal data offered by the UK and that can only be a positive thing.

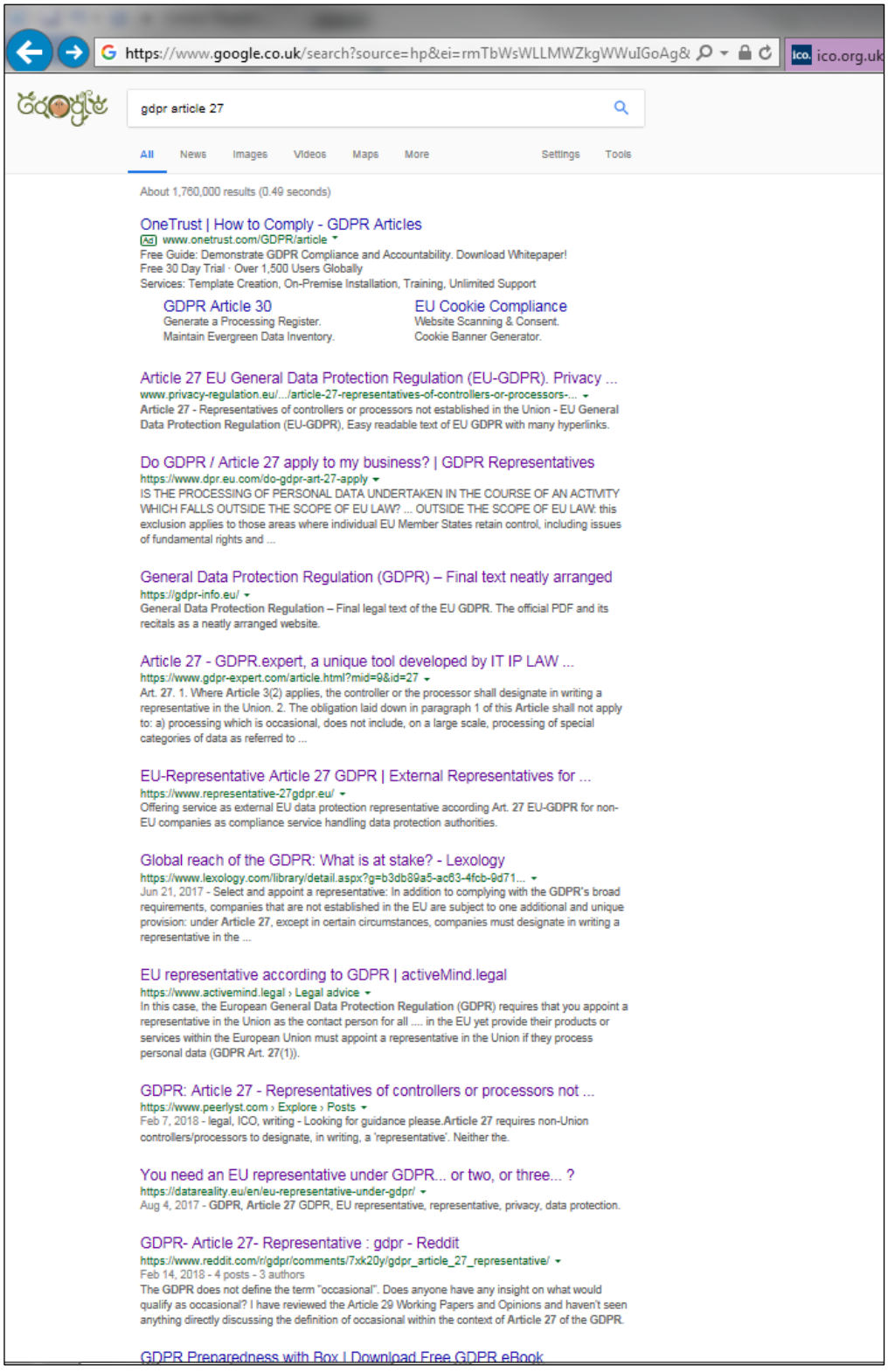
To close, the UK has been a driving force for data protection reform across the EU, reform whose reach is far beyond geographic boundaries. It is to be hoped the UK will

[262] House of Lords, 'Select Committee on the European Union, Home Affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (*parliament.uk* meeting date 8 March 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48744.html>
[263] C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650
[264] C-203/15 and C-698/15 *Tele2 Sverige AB and Others* [2016] ECLI:EU:C:2016:970
[265] ibid
[266] *R (on the application of the national council for Civil Liberties (Liberty)) v Secretary of State for the Home Department and another* [2018] EWHC 975 (Admin)
[267] Investigatory Powers Act 2016

continue to benefit from this reform and have a voice within it going forward. The importance to its own citizens as well as to those with whom the UK trades should not be underestimated at a time when the use of personal data has become more extensive than had been thought possible. The roots of data protection reach back to post-war Europe and the need to respect and evolve the rights that emerged from those dark times should be at the core of development; whether it be social, legal, economic or technological.

Appendix 1 - Results for Internet Search - Search term – "gdpr article 27"

Date 21 April 2018



Bibliography

Legislation

UK

Data Protection Act 1998

Data Protection Bill [HL] 2017-19

Data Retention and Investigatory Powers Act 2014

Investigatory Powers Act 2016

Regulation of Investigatory Powers Act 2000

Ireland

Data Protection Act 1998 as amended

European Union including Commission Decisions

Charter of Fundamental Rights of the European Union 2000/C 364/01

Charter of Fundamental Rights of the European Union 2012/C 326/02

Commission Decision 2016/2295 – amending Decisions 2000/518/EC, 2002/2/EC, 2003/490/EC, 2003/821/EC, 2004/411/EC, 2008/393/EC, 2010/146/EU, 2010/625/EU, 2011/61/EU and Implementing Decisions 2012/484/EU, 2013/65/EU on the adequate protection of personal data by certain countries, pursuant to Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council OJ L344 p 83 - 91

Commission Decision 2004/915/EC – amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries OJ L385 p 74 - 84

Commission Decision 2000/520/EC - pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [2000] OJ L215, p 7 - 47

Commission Decision 2003/821/EC - on the adequate protection of personal data in Guernsey [2003] OJ L308, p 27 - 28

Commission Decision 2016/1250 –pursuant to Directive 95/46/EU of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield [2016] OJ L207, p 1 - 112

Commission Decision 2010/87/EU – on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council OJ L39 p 5 - 18

Commission Decision 2001/497/EC –on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC OJ L181 p 19 - 31

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data OJ L281 p 0035-0050

Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201 p 0037 – 0047

Directive 2009/136/EC amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337 p 11 - 36

Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data [2016] OJ L119, p 0001-0081

Third Country

Data Protection (Bailiwick of Guernsey) Law, 2001

Data Protection (Bailiwick of Guernsey) Law, 2017

Cases

UK Courts

R (on the application of Davis MP and others) v Secretary of State for the Home Department [2015] EWHC 2092 (Admin)

R (on the application of Davis MP and others) v Secretary of State for the Home Department [2015] EWCA Civ 1185, [2015] AllER (D) 196

R (on the application of the national council for Civil Liberties (Liberty)) v Secretary of State for the Home Department and another [2018] EWHC 975 (Admin)

Court of Justice for the European Union

C-293/12 and C-594/12 *Digital Rights Ireland and Others* [2014] EU:C:2014:238

C-362/14 *Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650

C-203/15 and C-698/15 *Tele2 Sverige AB and Others* [2016] ECLI:EU:C:2016:970

Irish High Court

Data Protection Commissioner v Facebook Ireland Limited and another [2017] IEHC 545

Schrems v Data Protection Commissioner [2014] IEHC 310, 2013 765 JR

Journals & Articles

Given P et al, 'Brexit, the Great Repeal Bill and data protection law' (2017) PDP 17 6 (9)

Grest L, 'Brexit brainstorming: data privacy' (2016) 166 NLJ 7702, p17

Griffin N, 'Privacy v security' (2017) 167 NLJ 7732, p15

Huseyin R, 'News & Views – ICO gives guidance on changes to BCR applications' (2018) 18 2 (17)

Huseyin R, 'UK PM's Ambitious' data protection plan not unreasonable, say experts' (2018) PDP 18 4 (1) (2)

Huseyin R, 'UK seeks adequacy-style decision from EU' (2017) PDP 17 8 (1) (2)

Miller J, 'Planning for Brexit' (2016) 166 NLJ 7702, p5 (1)

Miller J, 'Safe harbour no more' (2015) 165 NLJ 7671, p4 (2)

Mourby M et al, 'Virtues out of necessity?' (2017) 167 NLJ 7771, p11

Mullock J, 'Brexit – a data protection perspective' (2016) PDP 16 6 (14)

Proops QC A, 'Brexit & the future of data protection' (2016) PDP 17 7(8)

Treacy B, 'Expert comment' (2017) PDP 17 8 (2)

Treacy B, 'Expert Comment' (2018) PDP 18 2 (2)

Treacy B, 'GDPR series: preparing for One Stop Shop' (2017) PDP 17 4 (7)

Watts V et al, 'Countdown to the GDPR begins' (2017) 40 CSR 12, 185

Books

Carey P, *Data Protection: A Practical Guide to UK and EU Law* (4th edn, OUP Oxford 2015)

Jay R, *Data Protection Law and Practice* (4th edition, Sweet & Maxwell 2012)

Jay R, *Guide to the General Data Protection Regulation* (1st edition Sweet& Maxwell 2017)

Websites

--, '32016R0679 – Factsheet outlining incorporation of Regulation (EU) 2016/679 into EEA Agreement' (*EFTA* no date) <www.efta.int/eea-lex/32016R0679> last accessed 18 March 2018

--, 'Agreement on the European Economic Area' (*EFTA* 1 August 2016) <www.efta.int/media/ documents/legal-texts/eea/the-eea-agreement/Main%20Text%20of%20the%20Agreement/EEAagreement.pdf> last accessed 19 March 2018

--, 'Annex XI Electronic Communication, Audiovisual Services and Information Society' (*EFTA* 09 February 2018) <www.efta.int/media/documents/legal-texts/eea/the-eea-agreement/Annexes%20to%20the%20Agreement/annex11.pdf> last access 18 March 2018

--, 'Bill stages – Data Protection Bill [HL] 2017 – 19 (*www.parliament.uk* no date) <https://services.parliament.uk/Bills/2017-19/dataprotection/stages.html > last accessed 05 May 2018

--, 'Binding corporate rules' (*ICO* no date) <https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/> last accessed 02 May 2018

--, 'CJEU gives judgment in DRIPA case' (*Landmark Chambers* 21 December 2016) <www.landmarkchambers.co.uk/news.aspx?id=4507> last accessed 28 April 2018

--, 'College Meeting : European Commission endorses provisions for data flows and data protection in EU trade agreements' (*European Commission* 31 January 2018) <http://europa.eu/rapid/press-release_MEX-18-546_en.htm> last accessed 28 April 2018

--, 'Commission decisions on the adequacy of the protection of personal data in third countries' (*European Commission*) <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> last accessed 29 May 2017

--, 'Communication from the Commission to the European Parliament and the Council – Exchanging and protecting personal Data in a Globalised World' (*European Commission* 10 January 2017) <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN> last accessed 16 April 2018

--, 'Data Protection' (*EFTA* no date) <www.efta.int/EEA/Data-Protection-505036> last accessed 18 March 2018

--, 'Data Protection Bill' (*ICO* no date) <https://ico.org.uk/for-organisations/data-protection-bill/> last accessed 27 September 2017

--, 'Data Protection Law Approved by UK Privy Council' (*gov.gg* 29 March 2017) <www.gov.gg/article/164773/Data-Protection-Law-Approved-by-UK-Privy-Council> last accessed 15 April 2018

--, 'Deadline to amend UK surveillance laws' (*BBC News* 27 April 2018) <www.bbc.co.uk/news/technology-43928147> last accessed 28 April 2018

--, EEA Joint Committee (*EFTA* no date) <www.efta.int/eea/eea-institutions/eea-joint-committee> last accessed 10 April 2018

--, 'Edward Snowden: Leaks that exposed US spy programme' (*BBC News* 17 January 2014) <www.bbc.co.uk/news/world-us-canada-23123964> last accessed 24 April 2018

--, EU Programmes with EEA EFTA Participation (*EFTA* no date) <www.efta.int/eea/eu-programmes> last accessed 10 April 2018

--, 'Europol and Brexit: Will UK retain access to EU intelligence sharing? (*BBC News* 20 September 2017) <www.bbc.co.uk/news/uk-41240643> last accessed 27 September 2017

--, 'Explanatory Memos on the litigation Concerning Standard Contractual Clauses – Explanatory Memo dated 28 September 2016' (*Irish Data Protection Commissioner* 26 September 2016) <https://dataprotection.ie/viewdoc.asp?DocID=1598&ad=1> last accessed 01 May 2018

--, 'General Data Protection Regulation' (*gov.gg* 16 September 2016) <www.gov.gg/gdprnews> last accessed 15 April 2018

--, 'Government to strengthen UK data protection law' (*GOV.UK* 07 August 2017) <www.gov.uk/government/news/government-to-strengthen-uk-data-protection-law> last accessed 16 September 2017

--, 'International data transfers using model contracts' (*European Commission* no date) <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en> last accessed 01 May 2018

--, 'Model Contract Clauses – International transfers of personal data' (*ICO* no date) <https://ico.org.uk/media/for-organisations/documents/1571/model_contract_clauses_international_transfers_of_personal_data.pdf> last accessed 01 May 2018

--, 'Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection' (*European Commission* 09 January 2018) <http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245> last accessed 15 January 2018

--, 'PM speech on our future economic partnership with the European Union' (*GOV.UK* 2 March 2018) <www.gov.uk/government/speeches/pm-speech-on-our-future-economic-partnership-with-the-european-union> last accessed 05 May 2018

--, 'Position paper on the Use of Data and Protection of Information Obtained or Processed before the withdrawal date' (*European Commission* 20 September 2017) <https://ec.europa.eu/commission/sites/beta-political/files/data_and_protection.pdf> last accessed 15 January 2018

--, 'Protocol 1 on Horizontal Adaptations' (*EFTA* 09 February 2018) <www.efta.int/sites/default/files/documents/legal-texts/eea/the-eea-agreement/Protocols%20to%20the%20 Agreement/protocol1.pdf> last accessed 18 March 2018

--, 'Queen's Speech: New data protection law' (*BBC News* 21 June 2017) <www.bbc.co.uk/news/technology-40353424> last accessed 17 September 2017

--, 'Resolutions Billet XXII 29 November 2017' (*gov.gg* 29 November 2017) <www.gov.gg/CHttpHandler.ashx?id=111064&p=0> last accessed 15 April 2018

--, 'The Bailiwick of Guernsey' (*gov.gg* no date) <www.gov.gg/article/120176/Information-on-the-location-of-the-islands-and-their-constitution> last accessed 15 April 2018

--, 'The Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018' (*gov.gg* no date) <www.gov.gg/CHttpHandler.ashx?id=112468&p=0> last accessed 17 April 2018

--, 'The electoral register and the open register' (*gov.uk* no date) <www.gov.uk/electoral-register/view-electoral-register> last accessed 16 April 2018

--, 'The eighth data protection principle and international data transfers' (*ICO* 30 June 2017) <https://ico.org.uk/media/for-organisations/documents/1566/international_transfers_legal_guidance.pdf> last accessed 16 April 2018

--, 'The European Free Trade Association' (*EFTA* no date) <www.efta.int/about-efta/european-free-trade-association> last accessed 10 April 2018

--, 'The EU in brief' (*European Union* no date) <https://europa.eu/european-union/about-eu/eu-in-brief_en> last accessed 04 February 2018

--, 'Theresa May: Human rights laws could change for terror fight' (*BBC News* 07 June 2017) <www.bbc.co.uk/news/election-2017-40181444> last accessed 17 September 2017

--, 'Transfers of personal data to third countries or international organisations' (*ICO* 17 August 2017) <https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/transfer-of-data/> last accessed 27 September 2017

--, 'Welcome to the Privacy Shield' (*Privacy Shield Framework* no date) <www.privacyshield.gov> last accessed 03 May 2018

--, 'What now for Brexit?: Post Election Briefing' (*Hogan Lovells* 09 June 2017) <www.hoganlovellsbrexit.com/latest-thinking/68/what-now-for-brexit-post-election-briefing> last accessed 17 September 2017

Article 29 Working Party, 'Adequacy Referential (updated)' (*European Commission* 28 November 2017) <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48827> last accessed 27 December 2017

Article 29 Working Party, 'Draft Guidelines on the accreditation of certification bodies under regulation (EU) 2016/679' (*European Commission* 6 February 2018) <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49877> last accessed 22 April 2018

Article 29 Working Party, 'EU – US Privacy Shield – First annual Joint Review' (*European Commission* 28 November 2017) <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782> last accessed 27 December 2017

Article 29 Working Party, 'Guidelines for identifying a controller or processor's lead supervisory authority' (*European Commission* 5 April 2017) <http://ec.europa.eu/newsroom/document.cfm?doc_id=44102> last accessed 27 December 2017

Article 29 Working Party, 'Guidelines on Article 49 of Regulation 2016/679' (*European Commission* 6 February 2018) <http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49846> last accessed 21 April 2018

Article 29 Working Party, 'Guidelines on Consent under regulation 2016/679' (*European Commission* 28 November 2017) <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849> last accessed 21 April 2018

Article 29 Working Party, 'Guidelines on Data Protection Officers ('DPOs') (*European* Commission 13 December 2016) <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048> last accessed 21 April 2018

Article 29 Working Party, 'Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive' (*European Commission* 24 July 1998) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf> last accessed 16 April 2018

Article 29 Working Party, 'Working Document – Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive' (*European Commission* 24 July 1998) <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf> last accessed 15 January 2018

Article 29 Working Party, 'Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers" (*European Commission* 3 June 2003) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf> last accessed 02 May 2018

Article 29 Working Party, 'Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules' (*European Commission* 29 November 2017) <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48798> last accessed 27 December 2017

Article 29 Working Party, 'Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules' (*European Commission* 29 November 2017) <http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48799> last accessed 29 November 2017

Brown R, 'UK firms won't be exempt from new EU data sharing rules – here's why' (*CNBC* 21 July 2017) <www.cnbc.com/amp/2017/07/21/uk-firms-wont-be-exempt-from-new-eu-data-sharing-rules--heres-why.html> last accessed 17 September 2017

Buttarelli G, 'The State of the Data Protection Union' (*EDPS* 20 September 2017) <https://edps.europa.eu/press-publications/press-news/blog/state-data-protection-union_en> last accessed 27 September 2017

Cerulus L, 'UK's data flows under EU surveillance' (*Politico* 24 August 2017) <www.politico.eu/pro/united-kingdom-brexit-data-flows-under-eu-surveillance/amp/> last accessed 17 September 2017

Department for Exiting the European Union, 'The exchange and protection of personal data - a future partnership paper' (*gov.uk* 24 August 2017) <www.gov.uk/government/publications/the-exchange-and-protection-of-personal-data-a-future-partnership-paper> last accessed 07 November 2017

Dipple-Johnstone J, 'Changes to Binding Corporate Rules applications to the ICO' (*ICO* 20 November 2017) <https://iconewsblog.org.uk/2017/11/20/changes-to-binding-corporate-rules-applications-to-the-ico/> last accessed 24 April 2018

EU Home Affairs Sub-Committee, 'The EU Data Protection Package' (*parliamentlive.tv* 1 March 2017) <www.parliamentlive.tv/Event/Index/d0004efc-f644-4383-bf01-9d860bbe78ee> last accessed 29 May 2017

Heimes R, 'Top 10 operational impacts of the GDPR: Part 9 – Codes of conduct and certifications' (*IAPP* 24 February 2016) <https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-9-codes-of-conduct-and-certifications/> last accessed 22 April 2018

HM Government, 'The United Kingdom's exit from and new partnership with the European Union' (*gov.uk* 2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/589189/The_United_Kingdoms_exit_from_and_partnership_with_the_EU_Print.pdf> last accessed 14 April 2018

House of Lords, 'Brexit: the EU data protection package' (*parliament.uk* 18 July 2017) <https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf> last accessed 14 April 2018

House of Lords, 'Select Committee on the European Union, Home Affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Rt Hon Matt Hancock MP, Minister of State for Digital and Culture' (*parliament.uk* meeting date 1 February 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/46835.html> last accessed 14 April 2018

House of Lords, 'Select Committee on the European Union, Home Affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Antony Walker, Deputy CEO, techUK; Ruth Boardman, Co-Head, International Data Protection Practice, Bird and Bird' (*parliament.uk* meeting date 1 February 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/49297.html> last accessed 14 April 2018

House of Lords, 'Select Committee on the European Union, Home Affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witnesses: Stewart Room, Partner, Global Cyber Security and Data Protection Legal Services leader, and UK Data Protection leader, PricewaterhouseCoopers LLP; Professor Valsamis Mitsilegas, Professor of European Criminal Law, Queen Mary University of London; Rosemary Jay, Senior Consultant Attorney, Hunton & Williams' (*parliament.uk* meeting date 1 March 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48742.html> last accessed 14 April 2018

House of Lords, 'Select Committee on the European Union, Home Affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Elizabeth Denham, UK Information Commissioner' (*parliament.uk* meeting date 8 March 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/48744.html> last accessed 14 April 2018

House of Lords, 'Select Committee on the European Union, Home Affairs Sub-Committee, Correct oral evidence: The EU Data Protection Package – witness: Baroness Williams of Trafford, Minister of States, Home Office' (*parliament.uk* meeting date 26 April 2017) <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-home-affairs-subcommittee/eu-data-protection-package/oral/69266.html> last accessed 14 April 2018

Hunt A et al, 'Brexit: All you need to know about the UK leaving the EU' (*BBC News* 30 January 2018) <www.bbc.co.uk/news/uk-politics-32810887> last accessed 4 February 2018

Kateifides A, 'UK: Data Protection Bill "adds extra layer of complexity" to GDPR' (*DataGuidance* 21 September 2017) <www.dataguidance.com/uk-data-protection-bill-adds-extra-layer-complexity-gdpr/> last accessed 27 September 2017

Lauchlan S, 'More lipstick for the Privacy Shield piggy as Eurocrats take data rhetoric to Washington' (*diginomica* 21 September 2017) <http://diginomica.com/2017/09/21/lipstick-privacy-shield-piggy-eurocrats-head-take-data-rhetoric-washington/amp/> last accessed 27 September 2017

Meyer D, 'Most member states won't be ready for GDPR' (*iapp* 24 April 2018) <https://iapp.org/news/a/most-member-states-wont-be-ready-for-gdpr/> last accessed 05 May 2018

Peter (Spiceworks), 'Most will miss GDPR deadline: UK most prepared, US and rest of EU lag behind' (*spiceworks* 02 May 2018) <https://community.spiceworks.com/blog/3023-most-will-miss-gdpr-deadline-uk-most-prepared-us-and-rest-of-eu-lag-behind> last accessed 05 May 2018

Stupp C, 'Commission conducting review of all foreign data transfer deals' (*Euractiv* 09 November 2017) <www.euractiv.com/section/data-protection/news/commission-conducting-review-of-all-foreign-data-transfer-deals/> last accessed 15 April 2018

Thomas K, 'Canada's national DPA to step up enforcement' (*Privacy Laws & Business* 22 September 2017) <www.linkedin.com/pulse/canadas-national-dpa-step-up-enforcement-k-an-thomas/?published=t> last accessed 27 September 2017

Ustaran E, 'GDPR – beyond the panic' (*Bloomsbury Law Online* September 2017) <www.infolaw.co.uk/newsletter/2017/09/gdpr-beyond-panic/> last accessed 27 September 2017

Ustaran E et al, 'UK's draft GDPR implementation law, the starting point' (*IAPP* 25 September 2017) <https://iapp.org/news/a/uks-draft-gdpr-implementation-law-the-starting-point/> last accessed 27 September 2017

Woodhouse J & Lang A, 'Briefing paper – Brexit and data protection' (*House of Commons Library* 10 October 2017) <http://researchbriefings.files.parliament.uk/documents/CBP-7838/CBP-7838.pdf> last accessed 18 March 2018

Glossary

Article 29 Working Party	Set up under Article 29 of the DP Directive – comprising representatives from EU Member States' data protection supervisory authorities – forerunner to the EDPB
BCRs	Binding Corporate Rules
CJEU	Court of Justice for the European Union
DP Directive	Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data OJ L281 p 0035-0050
DPA	Data Protection Act 1998
DRIPA	Data Retention and Investigatory Powers Act 2014
EDPB	European Data Protection Board – set up under Article 68 of the GDPR – comprising representatives from EU Member States' data protection supervisory authorities
EEA	European Economic Area – comprising the 28 EU Member States and three EFTA countries, Iceland, Liechtenstein and Norway
EEC	European Economic Community
EFTA	European Free Trade Association
EU	European Union
GDPR	General Data Protection Regulation - Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and the free movement of such data [2016] OJ L119, p 0001-0081
ICO	The Information Commissioner's Office, the UK data protection supervisory body
Irish DPC	Irish Data Protection Commissioner
RIPA	Regulation of Investigatory Powers Act 2000
The Charter	The Charter of Fundamental Rights of the European Union 2012/c 326/02
The Commission	The European Commission

The E-Privacy Directive	Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201 p 0037 – 0047
The Treaty	The Treaty of Lisbon
Third country	A country outside the EU
UK	United Kingdom