

No interruptions

Options for the future UK-EU
data-sharing relationship

November 2017



Acknowledgements and Contacts

This report was prepared by techUK and UK Finance with support from Dentons UKMEA LLP.

techUK

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. Over 950 companies are members of techUK, collectively they employ more than 700,000 people. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium-sized businesses.

techUK is committed to helping its members grow, by:

- Developing markets
- Developing relationships and networks
- Reducing business costs
- Reducing business risks.

Contacts: Antony Walker, Jeremy Lilley, Giles Derrington, Sue Daley, Alice Jackson

www.techuk.org

UK Finance

UK Finance represents nearly 300 of the leading firms providing finance, banking, mortgages, markets and payments related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and UK Cards Association. UK Finance has an important role to play helping negotiators understand how the interests of UK and EU customers and the financial services they all depend upon can be best protected. Our members are large and small, national and regional, domestic and international, corporate and mutual, retail and wholesale, physical and virtual, banks and non-banks. Our members' customers are individuals, corporates, charities, clubs, associations and government bodies, served domestically and cross-border. These customers access a wide range of financial and advisory products and services, essential to their data-to-day activities. The interests of our members are at the heart of our work.

Contacts: Ronald Kent, John Thompson, Matthew Field, Conor Lawlor, Diederik Zandstra, Andrew Rogan, Rebecca Park, Parisa Smith

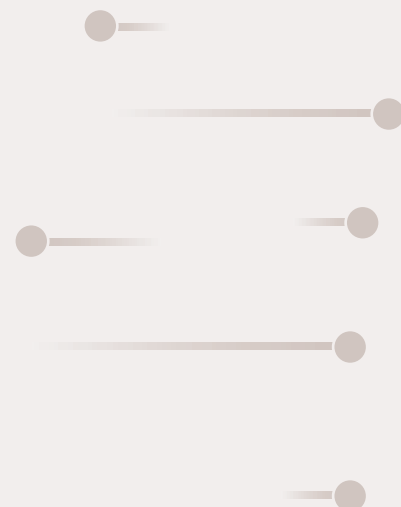
www.ukfinance.org.uk

Dentons UKMEA LLP

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognised by prominent business and legal publications for its innovations in client service, including founding Nextlaw Labs and the Nextlaw Global Referral Network. Dentons' polycentric approach and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.

Contact: Martin Fanning

www.dentons.com



“The adequacy standard does not require a point-to-point replication of EU rules. Rather, the test lies in whether, through the substance of privacy rights and their effective implementation, enforceability and supervision, the foreign system concerned as a whole delivers the required high level of protection. As the adequacy decisions adopted so far show, it is possible for the Commission to recognise a diverse range of privacy systems, representing different legal traditions, as being adequate.”

Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World

Contents

Foreword from techUK.....	6
Foreword from UK Financial Director.....	7
Executive Summary.....	8
Introduction.....	11
1 Why the Free Flow of Data Between the UK and the EU is Important and Must Continue.....	13
2 Ensuring the Free Flow of Data – What Options Exist?.....	21
3 The Mechanics of the Existing Data Adequacy Process – How it Works.....	25
4 Roadmap for UK – EU Adequacy.....	29
5 UK Government Proposal for the Exchange and Protection of Personal Data – August 2017.....	34
6 Onward Transfers from the UK and their Impact on Adequacy.....	36
Conclusion.....	39
Annex – Alternative bases for international data transfers.....	41
Frequently Used Terms.....	47
Glossary.....	48



Foreword from techUK

The United Kingdom's decision to leave the European Union has brought about many important and complex legal challenges. The need to put in place a clear legal basis to enable the lawful transfer of personal and sensitive data between the EU and the UK presents a difficult challenge, but not an insurmountable one.

“The biggest challenge is time”

Firstly, the interests of all parties in this issue should be aligned – consumers, businesses and governments in both the UK and the EU will all suffer costs and disruptions if this issue is not successfully addressed. Secondly, divisions on matters of substance are small – the UK and EU will in effect have remarkably similar legal frameworks for data protection. And finally, there are established processes and precedents for putting Adequacy arrangements in place between the EU and third countries with different legal approaches to the protection of personal data.

The biggest challenge is time. To put in place a new legal framework for cross-border data flows requires both parties to follow a robust procedure of due diligence in order to achieve a mutual adequacy decisions. This process normally takes a number of years to complete. The fastest adequacy decision reached by the European Union took 18 months. A quick glance at the Brexit clock makes it clear that time is running out.

The UK government has recognised the importance of this issue and earlier this year put forward an ambitious proposal for a bespoke data flows agreement with the EU based on the principles of mutual adequacy and enhanced cooperation. This proposal is interesting and, if successful, would secure the outcomes desired by businesses in the UK and across the EU. However, given that there is no precedent for a country leaving the EU it is difficult for businesses to judge the likelihood of such an approach being successful. Meanwhile, it seems highly likely that some matters of substance would have to be addressed regardless of whether the UK and EU chose to pursue a novel procedure or the more traditional adequacy process.

Should the UK and EU fail to agree a mutual adequacy arrangement, businesses and other organisations in both the UK and the EU27 would have to resort to putting in place burdensome, expensive and unstable legal mechanisms to enable the lawful transfer of personal data. This would cause significant disruption and would be a major drag on the trade of 21st century goods and services. As this report explains, this would be a terrible outcome for businesses and organisations of every size and in every sector. It would also cause disruption and uncertainty for the consumers.

Given the challenges of time and the risk of a “cliff-edge” it is essential that the UK and EU make rapid progress toward reaching mutual adequacy arrangements as soon as possible. This should be a top priority once negotiations are able to move on to the UK's future relationship with the EU. Transitional arrangements will, in-all-likelihood, be required as a bridge between the completion of the Article 50 process and the completion of the adequacy process. This report sets out some of the key issues that will need to be addressed and draws upon experience of similar negotiations that should be helpful for informing the process. No one should view the fall-back position of a no-deal scenario as an attractive option.

This report has been developed as a positive contribution to addressing one of the more arcane, but, nevertheless, far reaching consequences of the UK's decision to leave the European Union. Privacy and data protection are issues of huge significance in the modern world. It is in the interests of businesses and consumers that the UK and the EU continue to work closely to ensure high levels of data protection, common standards and consumer confidence in a modern digital economy.



Julian David, CEO techUK

Foreword from UK Finance

The United Kingdom's exit from the European Union will transform the way personal data is shared between the two parties from a relationship based on a deeply integrated single legal framework to one between two separate jurisdictions.

"We believe adequacy should be the framework for the continued protection and movement of personal data between the UK and EEA, but it will take time to put in place."

For millions of EU and UK citizens and businesses, and for billions of individual exchanges of personal data currently relying on a borderless environment, this will be a significant and potentially disruptive change. It will require a new relationship between two legal frameworks based on the mutual goal of ensuring a high standard of protection for citizens' personal data.

Citizens, businesses and organisations move personal data back and forth across national borders within the EEA as a normal part of their day-to-day activities. Banks share personal data for operational and financial crime purposes; academic organisations move data across borders for medical research; and many data centres sell the resources needed to move, store and analyse this data. When the UK leaves the EU, it will leave this relationship and, without another arrangement in place, transfers of personal data between the UK and EU could be severely disrupted and in some cases will be forced to stop.

This report is intended as a contribution to the debate about what that future relationship might look like and how it can be built in a way that preserves one of the major commercial and economic benefits of the existing close ties. It describes the options for that new relationship which could ensure that personal data remains protected but continues to move between the UK and the EEA as it does currently. Of those options, mutual adequacy agreements between the UK and the EU is the solution which best allows citizens, businesses and organisations to continue to enjoy the benefits and protections that they currently do. The solution is mutual because, once outside the EU, the UK will have the same need to authorise the movement of personal data between the UK and the EU as the EU will have between the EU and the UK.

We believe adequacy as the framework for the continued protection and movement of personal data between the UK and EEA has a number of advantages – it enables both sides to be sure that their citizens' personal data enjoys high standards of protection, it allows the UK and EU to continue to cooperate on the international stage in this area and it recognises the common value placed by both parties on the free flow of data as well as the fact that they are beginning from a point of legal harmony. In doing so, it also recognises that the UK outside of the EU Single Market cannot receive the privileges of a Single Market member and makes use of an established EU mechanism for delivering a pragmatic solution.

However, determining adequacy involves a legal process that will take time to put in place. The UK and EU must be realistic about this fact and work to avoid a "cliff-edge" in which the movement of personal data stops. This would be detrimental to the millions of citizens and hundreds of thousands of businesses that rely on this ability. We would encourage the EU and UK to agree to a standstill transitional arrangement for a set period of time to allow time for mutual adequacy agreements to be put in place.

A new framework for the protection and movement of personal data established on the foundations described in this report can contribute a key element in the positive, reframed and close relationship for the benefit of Europe and its 500 million citizens.



A handwritten signature in black ink, appearing to read 'Stephen Jones'.

Stephen Jones, CEO UK Finance

Executive Summary

Data and the modern EEA economy

In a modern economy the flow of data is an integral part of trade and business. Businesses hold the data of their customers and employees and use it to manage operations, customise and market services, fulfil orders and communicate in a wide range of ways. Consider:

- a clothing order from a consumer being fulfilled by an online retailer;
- a human resources department centralising employment records from a number of different operations;
- a big data start-up working on a vast dataset of information points from across a client's entire customer base; and
- a bank sharing data on an individual with its specialists in another location as part of anti-fraud checks.

From the examples above, it is immediately obvious how data transfers of this kind support trade and economic activity. What all of these activities have in common is that they involve the transfer of individuals' personal and sensitive data from one point to another via the internet for processing or other use. Such transfers are routine and ubiquitous across the EEA and describe in each case common forms of data transfer between the UK and the rest of the EEA.

Importantly, these data transfers often reflect structural features of a company's business model such as the physical location of data management centres or the centralisation of data management both for reasons of security and efficiency. These are arrangements that are rarely simple or cost-free to adapt or restructure.

In a modern economy the flow of data is an integral part of trade and business.

The other significant feature of such transfers is that they are tightly regulated in the EEA. They are rightly treated as requiring a very high level of data and privacy protection, as they involve individuals' personal details. The reason such flows are relatively simple inside the single market is because they are protected and policed by the EU's unified data protection regime. Even where the sender and receiver of data are in different EEA states, both states are bound by a common data protection framework and the transfer is treated as having taken place in a single jurisdiction. The new centrepiece of this regime is the General Data Protection Regulation (GDPR) which will apply from 25 May 2018.

Data transfer once the UK has left the EU

The transfer of such data becomes much more problematic when it takes place between the EEA and a state outside of the EEA. The GDPR prohibits the transfer of personal data to another country outside of the EEA under normal circumstances. The UK itself, having adopted the GDPR as domestic law, will have its own prohibitions on such transfers.

Unless agreed otherwise by the EU and the UK, at the end of March 2019, the UK will become a "third country" for data protection purposes. In simple terms, this means that from that date the UK will be a location which is not deemed by the EU to automatically offer sufficient safeguards and protections for EEA personal data and further steps will need to be taken by EEA exporters of personal data to ensure such data flows may continue on a lawful basis. The same is likely to be true in reverse in respect of transfers to the EEA from the UK. This poses a profound challenge for the kinds of data movements described above, which have become heavily integrated into the basic business models of companies and public-sector organisations operating between the UK and the rest of the EEA.

However, the GDPR contains various mechanisms for ensuring that such data transfers can take place between the EEA states and countries outside the EEA in defined circumstances.¹ One such is where the EU identifies that certain protections and safeguards are in place for the protection of personal data and deems a third country 'adequate'. A finding of adequacy assesses both the domestic protections for data protection in a third country as well as wider considerations, including the standards imposed on onward transfers of personal data from that country. Alternatively, the GDPR contains a number of limited derogations to the regulation where companies have put in place defined protections for personal data in their internal systems.

¹ If, as part of any post-March 2019 arrangement, the UK became part of the EEA, the UK would automatically be considered an 'adequate' destination for personal data. So long as the UK remained a member of the EEA, personal data would continue to flow to the UK from locations within the EEA without restriction (and vice versa) – as is presently the case for Iceland, Lichtenstein and Norway. (See GDPR Art. 44). Being a member of the EFTA would not bring the same status.

Transferring personal data at exit

In the absence of any adequacy decision between the UK and the EU – either on the model anticipated in the GDPR or in a bespoke agreement – companies will need to fall back on the alternative mechanisms contained in the GDPR.

These alternative mechanisms for businesses are:

- Binding Corporate Rules (BCRs);
- Standard Contractual Clauses (SCCs);
- Codes of Conducts;
- Certification Schemes; and
- Derogations in the law for specific situations.²

There are challenges, uncertainties, and disruptions associated with relying on such alternative bases for organisations in both in the UK and the EEA, especially for small to medium enterprises (SMEs).

In contrast, an adequacy decision is far preferred. It is universal, relatively simple and robust. It would create a shared structure of data protection practice between the EEA and the UK based on common high standards, and in doing so permit continued data flows between the EEA and the UK. A similar finding by the UK in respect of the EEA would have the same benefits. It would also be a sound basis for the EU and the UK to promote a culture of data protection best practice and openness globally.³

The UK Government has published a future partnership paper on the “Exchange and Protection of Personal Data”. The UK Government’s proposed approach to data protection envisages a bespoke arrangement, building on adequacy principles, recognising the close relationship both parties have on data protection. Under this arrangement the free flow of data between the UK and the EU would continue to be permitted and a role for the UK’s Information Commissioner’s Office (ICO) would be maintained at the European level. While the aims and objectives of the UK’s approach appear to be what industry desires, more detail is needed on how those aims will be achieved, particularly in the areas of timing, legal certainty and political risk.

The UK has strong arguments for adequacy as a country that has been at the heart of European data protection law for many years.

Adequate at exit?

The concept of adequacy reflected in the GDPR has been developed and amplified by recent CJEU case law, not least the October 2015 Schrems decision. As a result, any future adequacy assessment of the UK by the EU will not only evaluate UK data protection and privacy laws, but it will examine UK domestic law, including UK security law, and its international commitments to determine whether there is a level of protection of fundamental rights and freedoms that is “essentially equivalent” to that guaranteed by the EU. This concept of “essential equivalence” does not require identical law, but laws which offer the substantially same level of protection.

A GDPR adequacy assessment therefore considers a wide range of factors including domestic legislation, the independence of regulatory supervision and enforcement capacities of the regulator, the transparency of rights and the case law around their application. It also considers other international commitments that a third country has entered into, including its framework for onward transfer of personal data to other countries. This will be important in a UK-EU context, because the UK is a major centre for international data transfers, not least to the United States of America.

The process for securing a data adequacy judgement as set out in the GDPR is complex. It requires a detailed review by the European Commission, review by EU data protection supervisors and legislation implementing a positive EU decision if one is recommended. The decision is then subject to quadrennial review.

Given the time available under the Article 50 process, the fact that the GDPR does not apply until May 2018 and the legal complications posed by the UK’s unique status as an EU Member State subject to the Article 50 procedure, a full assessment of UK adequacy following normal procedures would appear difficult to complete by the end of the UK withdrawal negotiations.

Conversely, the UK has strong arguments for adequacy as a country that has been at the heart of European data protection law for many years, has been very active in the development of regulatory best practice and which will maintain the GDPR after exit.⁴

Nevertheless, this case is not clear cut: any “essential equivalence” assessment of the UK is likely to consider governmental surveillance powers and information-gathering activities, in particular under the Investigatory Powers Act 2016 which may be in tension with the GDPR as interpreted under the Charter of Fundamental Rights. Perhaps mindful of these challenges, the UK Government’s Data Protection Bill includes a distinct data protection framework for national security purposes, based on Convention 108 which is currently being revised.

² See GDPR Art. 49

³ See COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL “Exchanging and Protecting Personal Data in a Globalised World” COM (2017) 7 final

⁴ See the Data Protection Bill at https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/lbill_2017-20190066_en_1.htm. In the UK Government’s August 2017 “Statement of Intent” on the Data Protection Bill and its planned reforms, the UK explains that the proposed Data Protection Bill must be consistent with (i) the GDPR; (ii) the Data Protection Law Enforcement Directive; and (iii) the Council of Europe Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (“Convention 108”).

Transitional measures for data protection and beyond

For the reasons summarised above, it will be difficult to achieve a full adequacy decision from the European Commission (and reciprocally from the UK) during the Article 50 negotiation window. This raises the clear risk that the legal basis for numerous data transfers between the EEA and the UK will lapse completely overnight in March 2019 for thousands of exposed companies and their customers (the “cliff-edge”). Given the complexity of restructuring data flows of these businesses, and their ability to put in place alternative safeguards, this is matter of urgent concern.

Consequently, it is strongly recommended that the EU and the UK agree a transitional mutual adequacy solution for the UK and EEA as part of any UK withdrawal arrangements. The most straightforward mechanism would be to prolong the *acquis* for a time-limited period. Alternatively, an interim mutual adequacy determination (or similar special status) could be included within any Withdrawal Agreement (or as part of any ancillary or flanking bilateral agreement linked to the finalised withdrawal arrangements).

A further benefit of a transitional period would be to use this as an opportunity to negotiate and agree mutual data protection adequacy between the EU and the UK as part of a new, longer-term trade and cooperation framework or on a standalone basis.

To arrive at the recommended position of mutual adequacy, key steps need to be undertaken as a priority. In the UK:

- Alignment of UK Data Protection Law with the GDPR: passage of the UK Data Protection Bill into law as quickly as practicable and confirmation of the continuation of the GDPR framework after exit as anticipated by European Union (Withdrawal) Bill. The UK should pursue only derogations compatible with continued adequacy under the GDPR framework.

- Clear provisions in UK legislation permitting a UK finding of adequacy for third countries with a clear confirmation of the basis on which the UK will conduct third country assessments pursuant to UK GDPR – ideally by pursuing a model and a process which is consistent with (and follows) existing EU adequacy decisions.

In the UK-EU negotiation:

- Agree a standstill transitional arrangement with the EU for a set period that avoids a “cliff-edge” in the ability of personal data to move between the UK and EEA.
- Acceleration of EU commencement of a full UK adequacy assessment (and of UK commencement of a full EEA adequacy assessment) to be embedded in a future bilateral agreement or activated in a standalone form at the end of a transitional period. This should be robust and transparent and undertaken in a way to provide stakeholders on all sides with complete confidence in the new framework.
- Agreement between the EU and the UK that during the transitional period it is both appropriate and desirable for the UK to pursue adequacy agreements with third countries in sufficient time to ensure that they are in place to reinforce or underpin any mutual adequacy agreement with the EU. As a priority, a UK-US Privacy Shield dialogue should also be commenced in a way that is consistent with, and which does not undermine, the wider EU-US relationship on data privacy and data transfer.

The EU and the UK should also work to embed continued and robust regulatory cooperation on data protection in their future relationship. This could, for example, include close cooperation between the UK’s Information Commissioner’s Office and EU regulatory bodies. A mutual adequacy model, such as the one suggested in this report, would preserve the strong working relationships already in place and offer businesses further regulatory certainty. It would also create the platform for a strong EU-UK position in the global debate on data protection and the free flow of data in the global economy.

Key recommendations: the need for a future data-sharing relationship to prevent disruption and enable growth.

The main recommendation of this report is that the EU and UK should pursue mutual adequacy agreements to provide a legal framework for the movement of personal data between the two jurisdictions.

This outcome requires the following actions:

- | | | |
|--|---|---|
| • Both the EU and the UK should begin their adequacy assessment processes as soon possible. | • The UK should consider implementing additional measures to ensure that any EU concerns about the UK’s data protection framework are addressed, particularly regarding processing of data for UK national security purposes. | • The UK should ensure that its ‘onward transfer’ regime, including with the US, provides equivalent levels of protection to those set out in the EU’s regime as this will form a key part of the EU’s adequacy assessment. |
| • A standstill transitional arrangement for a set term in order to avoid a “cliff-edge” in the movement of personal data should be agreed immediately. | | |

Introduction

Data is global

The flow of personal data between the EEA and the UK is fundamental to the EEA's and UK's increasingly digitised, information-driven, economy and society. It also has profound effect on the way consumers conduct their lives. The UK's exit from the EU will have significant impacts on the basis under which personal data flows between the UK and EEA.

Currently, personal data flows between the UK and the EU in a myriad of ways. UK and EU citizens share personal data with each other across platforms; businesses gather information that helps them better reach their customers; researchers and universities conduct scientific study based on sharing personal data collected in one place and analysed in another; and governments and businesses use personal data to fight crime.

As the economic and social importance of data processing, storage and transfer has increased over the past twenty years, this has been matched by a growing need to protect citizens' fundamental rights and ensure that individuals are properly informed, consulted and provide consent for how their personal data is used. The EU and the UK have pioneered the development of online privacy rights which both provide protections for individuals and a reliable legal framework for businesses to innovate and operate under. As regulatory approaches of data transfers diverge globally, the importance of maintaining common standards and approaches in this area is becoming increasingly important.

If barriers to the flow of personal data arise where these did not previously exist, either deliberately or by omission, then this risks adverse consequences for societies and economies. Barriers to the free flow of personal data constrain growth, impede innovation, undermines data protection standards and reduce public outcomes on welfare, health and security. Such barriers will arise as the result of the UK's exit from the EU unless timely action is taken.

What Brexit means for data

On Friday 29 March 2019, the UK will leave the EU. Today, as a member of the EU, the UK is part of the same data protection regime as all other EEA Member States. Personal data can be moved seamlessly between all EEA Member States securely and under a high level of data protection. Depending on the exact nature of the UK's exit, these critical data flows will be put at risk.

Leaving the EU and not joining the EEA will move the UK outside of the formal EU data protection framework, making the UK a third country. For governments, public bodies, and businesses in the UK and EEA that exchange personal data, the UK becoming a third country presents a significant, yet not insurmountable, challenge to the future of the free flow of personal data between the UK and the EEA.

Finding the mutual benefit

This cross-industry report will assess the options available to the UK and EU to ensure the continued free flow of personal data and common high level of data protection. In making such an assessment it is important to remember that this is a period in which the personal data protection regime in the EEA is undergoing considerable change. Data protection laws in the EEA, and in the UK, are going through change with the new EU General Data Protection Regulation (GDPR) taking effect from 25 May 2018, roughly halfway through the Article 50 Brexit negotiation process.

The UK Government has introduced the Data Protection Bill, which sets out reforms to the UK's data protection framework, in line with GDPR, and the Data Protection Bill has begun the Parliamentary process. As a consequence, the data protection regimes in place in both the UK and EU will be aligned by the time the UK actually leaves the EU.

In addition to reflecting the material changes to data protection laws, any assessment must also take into account the wider context of Brexit negotiations. At the time of writing there remains considerable uncertainty regarding whether and when it may be determined that sufficient progress has been made in the UK and EU negotiations on withdrawal issues to move on to future relationship discussions.

What this report will cover

This report will consider the options that exist to ensure the free flow of data and a common approach to data protection between the UK and EEA. It will also explore timing considerations and the need for regulatory certainty. Organisations on both sides of the channel need certainty about the legal basis on which their international data transfers will be based. That certainty is needed sooner rather than later given the important operational decisions that will need to be taken in the coming months in order for them to continue providing the services they currently do at the standards expected by citizens in the UK and EEA.

The report will explain that the most compelling option currently available to preserve personal data flows is a mutual adequacy agreement.

The report will explain that the most compelling option currently available to preserve personal data flows is a mutual adequacy agreement. Such an agreement appears to be the most stable and legally secure mechanism to maintain the free flow of data between the UK and EU. The European Commission has an established process whereby it can determine a third country adequate based on an assessment of their data protection laws.

Adequacy assessments can take a considerable amount of time – the fastest assessment currently in force took approximately 18 months – and given the Article 50 window is narrowing, transitional arrangements are likely to be required to avoid a “cliff-edge” for businesses. Businesses will require early sight of any such transitional arrangements, which should guarantee the current ability to move personal data between the UK and EEA.

The report also considers the fall-back options in the scenario where no deal is reached. In such an event, businesses would have to rely on various narrow, unsuitable, burdensome and expensive legal mechanisms to ensure they can continue to transfer data between the UK and the EU. These fall-back bases (which are described elsewhere in this report) would not provide the certainty and clarity that businesses on both sides of the channel need to continue providing services to their customers, and would not be practical to implement for many small and mid-sized businesses.

The UK Government has published a future partnership paper on the “Exchange and Protection of Personal Data”.⁵ The UK Government’s proposed approach to data protection

envisages a bespoke arrangement recognising the close relationship both parties have had on data protection over the years. Under this arrangement the free flow of data between the UK and the EU would continue to be permitted and a role for the UK’s Information Commissioner’s Office (ICO) would be maintained at the European level. While the aims and objectives of the UK’s approach appear to be what industry desires, more detail is needed on how those aims will be achieved, particularly in the areas of timing, legal certainty and political risk.

Finally, the report puts the future of UK-EU data flows in the context of wider international data transfers with other third countries, both those already deemed adequate by the European Commission and those that are not. These so-called ‘onward transfer’ considerations will be a crucial element of any UK-EU deal for a future data-sharing relationship.

We live in a time of considerable change and some uncertainty in data protection regimes. It may be that some elements of this report are superseded or become out of date in the coming months. What will not change is the importance of securing the future of data flows on a stable and legal basis to the benefit of consumers, businesses and other organisations in the UK and EU. This report therefore sets out the options available, at the current time, to ensure that free flow of data can continue.

Transitional arrangements are likely to be required to avoid a “cliff-edge” for businesses.

GDPR – The EU’s Data Protection Regime

Within the EEA individuals have a fundamental right to the privacy and protection of their personal data. Personal data is any information relating to an identified or identifiable individual. Within the EEA, the movement of personal data is governed by the EU data protection regime, which permits intra-EEA transfers. The EU Data Protection Directive (DPD) sets out the minimum requirements that national data protection laws must have for collecting, accessing, storing, processing, and transferring the personal data of individuals in order to protect their fundamental rights and freedoms, including their right to data protection and privacy. Companies that comply with these data protection laws are free to transfer the personal data of customers, employees, vendors, business partners, and other individuals throughout the EEA.

However, the EU data protection framework is currently being revised and the DPD will be replaced in May 2018 when the new EU GDPR takes effect, after having been passed into law on 25 May 2016.

The introduction of GDPR is the biggest change to European data protection law in over twenty years and will impact governments, public bodies, businesses and individuals. The GDPR expands the definition of personal data which means that more types of information will be considered per se personal data and thus brought into scope of requirements around the transfer of that data.

The GDPR introduces tighter controls and requirements for businesses in many areas and builds upon the DPD by continuing to harmonise aspects of EU data protection law at the EU level. It continues to allow personal data to move freely between companies or other organisations in the EEA provided they respect these common EU standards.

The UK Government has committed to maintaining the GDPR following the UK’s exit, creating certainty over the data protection regime in place when the UK leaves the EU.

⁵ See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

1 Why the Free Flow of Data Between the UK and the EU is Important and Must Continue

Data flows between the UK and the other members of the EEA contribute significant value to the economies and societies on both sides of the Channel. Personal data can flow, without additional safeguards, throughout the EEA under current and incoming EU data protection rules.

Not only does this benefit hundreds of thousands of businesses and millions of individual customers, but also ensures that individuals across Europe enjoy high levels of protection and privacy for their personal data. All are potentially affected by the UK's exit from the EU. Suddenly losing the free flow of data would create a damaging "cliff-edge" effect. Both the UK and the EU thus have an interest in ensuring that an orderly and timely solution is found to ensure there is no gap in the ability of UK and EEA businesses, consumers and organisations to transfer data across jurisdictions.

In this chapter, we outline the complexity of UK and EEA data flows, and the economic and social importance of ensuring the frictionless ability of data to continue to flow between the UK and the EEA after the UK's exit to deliver benefits for both jurisdictions using examples in the fields of:

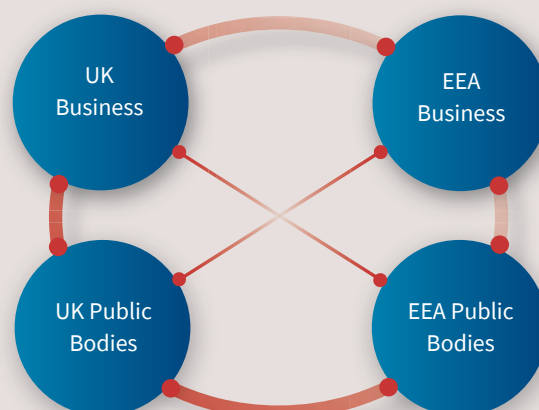
- **commerce and trade;**
- **the prevention of financial crime; and**
- **biomedical research.**

Complexity of UK and EEA data flows

The free flow of data underpins and impacts upon the day-to-day activities of nearly every UK and EEA individual, business, and institution. These data flows are increasingly multi-lateral and complex and occur on a horizontal, vertical, and diagonal basis, often in near real-time, as explained below:

- **Horizontal** – Data sharing between comparable bodies in different countries (e.g., UK/EEA business to UK/EEA business; UK/EEA public body to UK/EEA public body);
- **Vertical** – Data sharing between businesses and public bodies in the same country (e.g. UK business to UK public body; EEA business to EEA public body); and
- **Diagonal** – Data sharing between business and public bodies in different countries (e.g., UK/EEA business to UK/EEA public body; UK/EEA public body to UK/EEA business).

Movement of personal data in the UK and EEA



We need to work for a Europe that empowers our citizens and our economy. And today, both have gone digital. Digital technologies and digital communications are permeating every aspect of life.

President Juncker, State of the European Union speech, 14 September 2016.⁶

Commerce and trade – data the driver of growth

Data is fundamental to all sectors and industries and is estimated to be worth €739 billion to the European economy by 2020, representing 4% of overall EU GDP.⁷ It should be remembered at this point that the GDPR expands the definition of personal data. Therefore, while not all data is personal data, it is increasingly difficult to distinguish between personal and non-personal data when discussing global data flows, and the value that is derived from those flows. As the European Commission noted in its Communication on ‘Exchanging and Protecting Personal Data in a Globalised World’ ‘The internet and digitisation of goods and services has transformed the global economy and the transfer of data, including personal data, across borders is part of the daily operations of European companies of all sizes, across all sectors.’⁸

Economic growth is being driven by companies in sectors including retail, media, automotive, advertising and transport, using data to deliver increasingly personalised products, goods and services to both businesses and consumers and the development of a thriving data market. Businesses established across Europe such as Spotify (Sweden)⁹, Lego (Denmark)¹⁰, BMW (Germany)¹¹, AXA (France)¹², Telefonica (Spain)¹³ and John Lewis (UK)¹⁴ are already using data-driven technologies to deliver personalised and responsive real-time services wanted by UK and EEA consumers and businesses that also increase customer interaction and loyalty as well as reduce costs and increase operational efficiency. The use of data is also helping companies, including SMEs, be more responsive to customers by allowing a real-time view of the organisation’s operations and supply chain efficiency, enabling smart manufacturing and infrastructure as well as providing instantly operational cyber security.

As well as underpinning the digital transformation across traditional sectors and industries, data is a key driver of digital technological innovation and entrepreneurialism, estimated to be worth £66 billion in new business opportunities in the UK alone.¹⁵

Looking ahead, the next wave of the digital revolution is being powered by technologies including the Internet of Things (IoT), Robotics and Artificial Intelligence (AI), all of which have data at their core. The realisation of the full economic opportunities to consumers and businesses offered by technological innovations, such as driverless vehicles and autonomous intelligent machines, will only be possible if data is able to move unhindered across borders. The UK is in a central position to facilitate these global data flows – the UK accounted for 11.5 per cent of global cross-border data flows in 2015, compared with 3.9 per cent of global GDP and 0.9 per cent of global population. Significantly, 75% of these data flows are with EU Member States.¹⁶

Data especially underpins trade between the UK and the EU. Information is continuously shared as part of the £381.6 billion in annual trade between the UK and the EU and the UK is fundamental to the transatlantic movement of data, the largest such movement on the planet.¹⁷ Once the UK exits the EU, the UK will then become the EU’s third largest trading partner, after the United States and China.¹⁸ Put simply, trade and data go hand in hand. Whatever the UK and EU’s future trading relationship will look like, a deal that allows personal data to continue to move between the two economies will be crucial to making two-way trade deals continue to grow in volume and value.

6 See <https://publications.europa.eu/en/publication-detail/-/publication/c9ff4ff6-9a81-11e6-9bca-01aa75ed71a1/language-en/format-PDF/source-30945725>

7 See European Commission, Digital Single Market: Building a European data economy at <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy>

8 See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, available at https://ec.europa.eu/newsroom/document.cfm?doc_id=41157

9 See Forbes at <https://www.forbes.com/sites/bernardmarr/2017/10/30/the-amazing-ways-spotify-uses-big-data-ai-and-machine-learning-to-drive-business-success/#523fe6964bd2>

10 See Fortune at <http://fortune.com/2016/02/17/lego-diversity-digital/>

11 See BMW at <https://www.bmw.com/en/topics/fascination-bmw/connected-drive/bmw-cardata.html>

12 See At Internet at <https://blog.atinternet.com/en/video-interview-digital-analytics-data-science-at-axa/>

13 See Telefonica at <https://www.business-solutions.telefonica.com/en/products/big-data/data-services/strategy-transformation/>

14 See IT Pro Portal at <https://www.itproportal.com/news/john-lewis-why-operational-intelligence-can-be-the-key-to-ecommerce-success/>

15 ‘Data equity: unlocking the value of big data.’ Centre for Economics and Business Research’ White Paper, 4: 7–26

16 See Frontier Economics, The UK Digital Sectors After Brexit , p.10 at <http://www.frontier-economics.com/documents/2017/01/the-uk-digital-sectors-after-brexit.pdf>

17 See HMRC December 2016 statistics available at <https://www.uktradeinfo.com/Statistics/OverseasTradeStatistics/Pages/ArchiveOTS.aspx>

On the volume of transatlantic data flows see McKinsey Global Institute (2016), Digital globalization: The new era of global flows, p.30ff, <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>

18 See, European Commission statistics available at http://trade.ec.europa.eu/doclib/docs/2006/september/tradoc_122530.02.2017.pdf

“The ability to move data across borders has also become central to trade. About half of all trade in services is enabled by digital technologies and the associated data flows.¹⁹ The UK is a leading exporter of services globally, second only to the US, with services accounting for 44% of the UK’s total global exports.²⁰ Cross-border data flows in and out of the UK increased 28-fold between 2005 and 2015 and are expected to grow another five times by 2021. Three-quarters of the UK’s cross-border data flows are with EU countries.²¹”

House of Lords European Union Committee, *Brexit: the EU data protection package* (18 July 2017) <https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf>

Case study: data centres

Data centres provide the core digital infrastructure that underpins digital interactions by storing, managing, processing, receiving and transmitting digital data at scale. They are the agents of growth for the UK’s internet economy which contributes 10% of UK’s GDP, and an estimated £225 billion to the overall economy.²²

Data centres stimulate a complex, high value-add supply chain and enable multiple layers of economic activity. For example, a single data centre can provide IT functions for hundreds or even thousands of businesses, thus improving productivity and generating employment and growth within the data centre’s customer base.

There are good reasons why firms would choose to store their data in data centres located in other jurisdictions with high data protection standards, for instance in the UK from mainland Europe. For regulated industries, it is desirable from an operational risk perspective to maintain backup systems in different regions in order to mitigate the risk posed by natural disasters or unforeseen incidents. For this reason many data centre and infrastructure operators

have located in the UK and there is substantial use of data centres in the UK by firms operating in other EEA states, and in other EEA states by UK firms.

The data centre sector is also a major business success story in its own right. There are around 500 data centres in the UK. Roughly a third of these are colocation (commercial) facilities, operated by companies like Equinix, Pulsant, DigitalRealty, Global Switch, Virtus, etc. The remainder are split between ICT service providers (such as IBM, BT, Atos, Fujitsu, HPE) and “in house” facilities, directly supporting corporate IT functions for all sorts of organisations, for example universities, banks, and supermarkets.

Due to the accelerating demand for digital data, the London data centre market is the second largest in the world and a significant exporter of digital services such as data hosting and processing to customers around the world.²³ The UK data centre sector also acts as the entry point to the rest of Europe for many global data-dependent businesses.

¹⁹ See Frontier Economics, *The UK Digital Sectors After Brexit* at <http://www.frontier-economics.com/documents/2017/01/the-uk-digital-sectors-after-brexit.pdf> p.10

²⁰ See HSBC, *Unlocking the Growth potential of Services Trade*, p.6 https://globalconnections.hsbc.com/grid/uploads/trade_in_services.pdf

²¹ See Frontier Economics, *The UK Digital Sectors After Brexit*, p.10 at <http://www.frontier-economics.com/documents/2017/01/the-uk-digital-sectors-after-brexit.pdf>

²² See techUK, *Silver Linings: The Implications of Brexit for the UK Data Centre Sector*, p.4 at <https://www.techuk.org/insights/reports/item/9554-silver-linings-the-implications-of-brexit-for-the-uk-data-centre-sector>

²³ See CBRE (2017) *Europe Data Centres, Q2 2017* and CBRE (2017) *U.S. Data Centre Trends Report, H1 2017*

The introduction of actual (or the potential threat of) barriers to the movement of personal data could inhibit trade between the UK and the other members of the EEA, raising costs and red-tape for businesses – particularly SMEs – and consumers resulting in slower economic growth. These could include macro, or structural, factors as set out in the following examples:

- **Disruption to existing product and service supply chains** – for example in the automotive sector, personal data may need to flow across several European borders with a car part to allow an after-sales query or diagnostics process to be completed.
- **Impact on infrastructural investment** in data centres and associated network infrastructures in the UK and the EEA (with related downstream impacts on employment and dependant supply chain businesses). For SMEs the potential requirement to “lift and shift” data processing systems and infrastructure from one jurisdiction to another, or duplicate across multiple jurisdictions, will result in significant business costs and disruption.
- **Creation of uncertainty and operational risk that stalls innovation** in the development and delivery of cutting edge data-driven products and services by UK and EEA businesses and prevents access to these goods and services by UK and EEA customers.
- **Concerns around access to skilled** talent needed for UK and EEA companies to realise the full benefits of a data economy. Every advanced country is in a race for the skills and talent required to work on digital, and the talent pool is highly mobile. For example foreign born workers account for 18.4% of employment in the digital sector in the UK.²⁴ However, in the event of there being disruption to data flows, this does not mean that all of this talent, or even the UK skilled workforce will simply shift to other countries. Disruption in the UK and EEA data economies that leads to less data-driven innovation and economic growth could result in skilled talent moving to other global locations such as the US and Asia. This would contribute to a digital skills gap in the UK and EEA.

As we look ahead to an increasing data-driven IoT and AI-enabled future, businesses and citizens stand to benefit from UK and European innovation and creativity in these fields. However, this will only be possible if data, including personal data, can continue to flow and move between the UK and the EEA as it does today. Hindered data flows will not necessarily mean innovation doesn’t happen, but it may mean that such innovation happens elsewhere in the world, potentially as a result of heightened legal requirements for data transfer, increased business costs or a lack of skilled talent. These economic inhibitions and increased cost bases may also result in increased costs to consumers at a time of relatively low economic growth.

It is essential that EU businesses grasp the opportunities of digital technology to remain competitive at global level, that EU start-ups are able to scale up quickly, with full use of cloud computing, big data solutions, robotics and high-speed broadband, thereby creating new jobs, increased productivity, resource efficiency and sustainability.

– COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the Mid-Term Review on the implementation of the Digital Single Market Strategy, A Connected Digital Single Market for All, p.3 (10 May 2017) http://ec.europa.eu/newsroom/document.cfm?doc_id=44527

Financial services

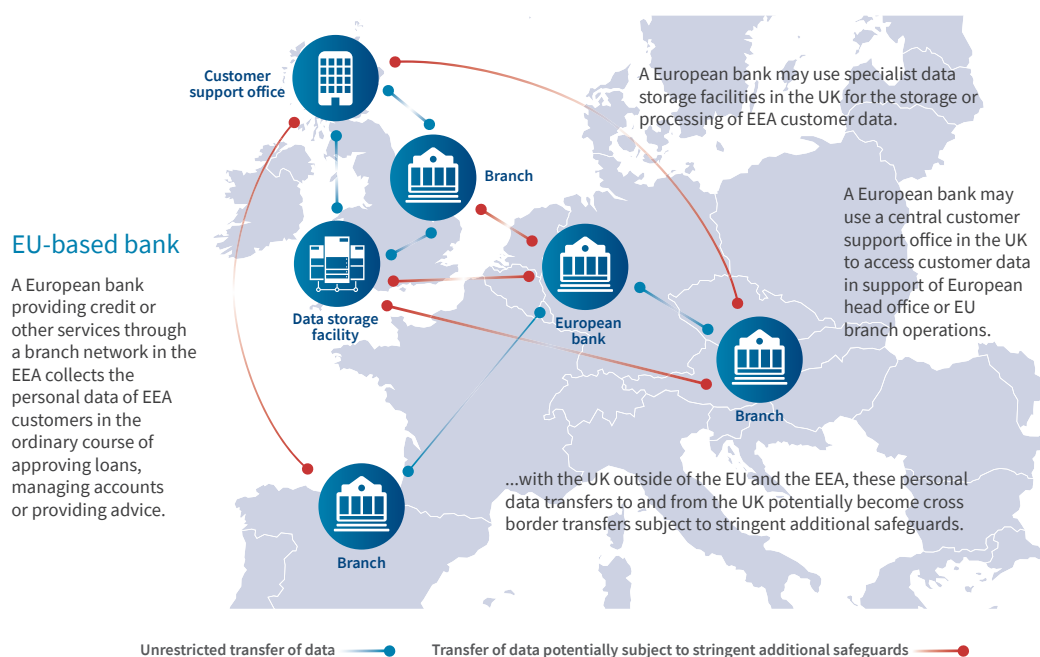
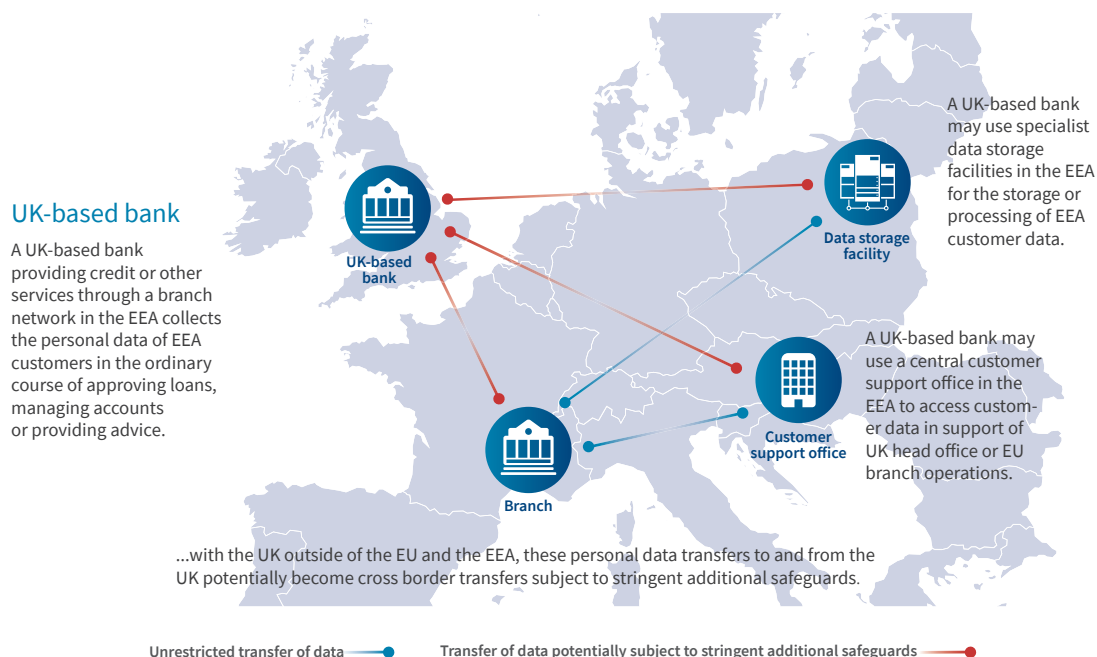
The movement of personal data between locations is an integral part of modern finance operations, both for established institutions and new start-ups operating in the FinTech space. Financial services firms store and process personal data digitally as part of conducting business, including operating retail and corporate accounts, providing lending, securities operations, investments, undertaking research and development, preventing financial crime and as part of workforce management.

If the UK is to continue to trade with the EU or to cooperate on law enforcement after it leaves, then it would seem preferable to have mechanisms in place beforehand for third country transfer. It also seems clear that either an adequacy decision or an international data-sharing agreement would best provide the “uninterrupted” and “unhindered” flow of data which the Government seeks

– European Scrutiny Committee, UK Parliament, Exchanging data with non-EU Countries (10 March 2017) <https://publications.parliament.uk/pa/cm201617/cmselect/cmeuleg/71-xxxii/7108.htm>

²⁴ See Frontier Economics, The UK Digital Sectors After Brexit , p.34 at <http://www.frontier-economics.com/documents/2017/01/the-uk-digital-sectors-after-brex-it.pdf>

Transfer of data across and outside of the European Economic Area (EEA)



Case study: Time critical information sharing

Organised criminals and terrorists do not respect borders and often they intentionally leave small footprints in different territories anticipating that no one territory can put the pieces together to reveal the big picture.

For example, an organised crime gang may carry out illegal activity in one territory and mask the funds generated through a business that is located in another territory. Once those funds have been introduced into the financial system, they are moved at speed and often outside the EEA. The gangs' methods make it difficult for financial institutions

and law enforcement to assemble the pieces to detect, prevent and disrupt activity unless information can be moved between them at speed across borders.

Further, a terrorist atrocity committed in one territory may be preceded by precursor activity in another territory and to avoid capture, movement across territories. The frictionless cross-border transfer of information between financial institutions and law enforcement agencies is the only way of ensuring that the pieces are put together in a time critical environment.

Financial crime: anti-fraud, money laundering, and terrorist financing

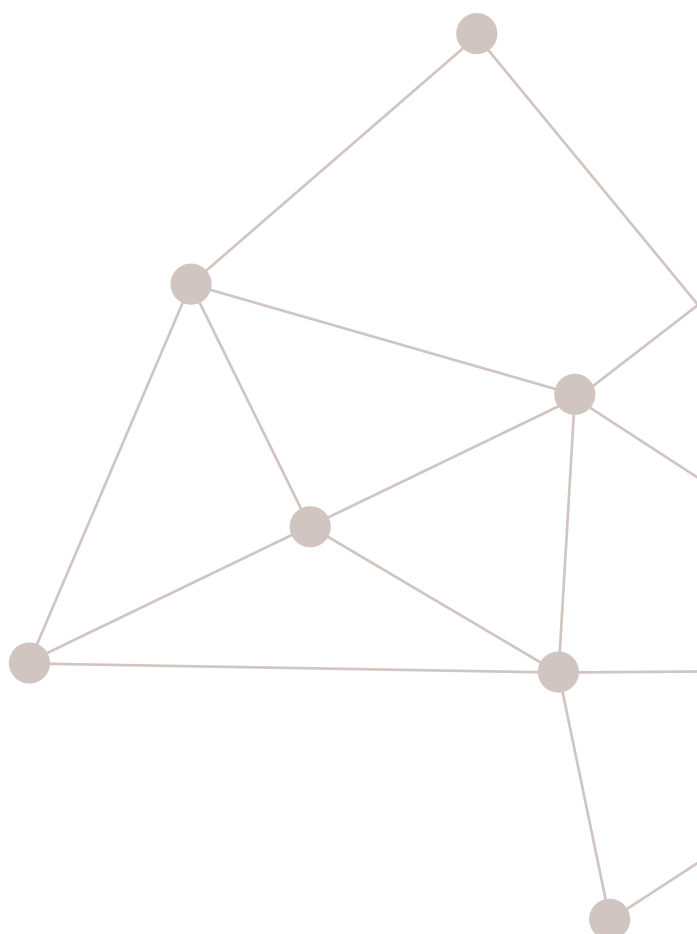
Organised crime and terrorism is increasingly global and cross border in nature. The UK and the EU already work closely to tackle shared issues such as fraud, money laundering, terrorist financing and tax evasion as these are issues which no one country has the information or ability to tackle alone. These are not insignificant issues. Presently, the United Nations Office on Drugs and Crime estimates that between 2% and 5% of global GDP is laundered each year – estimated to be between EUR 715 billion and EUR 1.87 trillion.²⁵ An effective money laundering operation relies upon a complex network of interconnected parts to collect, hide, and transfer money.²⁶

Nearly all organised crime in the EU will have a cross border element to it, be it flows of illegal goods, people or illicit funds.²⁷ Law enforcement cannot detect or prevent these threats alone without working with the private sector, particularly the financial sector which is the most vulnerable sector to money laundering for criminal and terrorist activities (for example, with criminals using the financial system to transfer funds).²⁷ In order to combat those threats, financial institutions must be able to share information with both law enforcement and also need to be able to share information across EU borders within their own institutions and with other parts of the regulated sector about threats, risks and suspicions.

This principle of needing to identify, understand and mitigate the threat is well understood and sits at the very heart of international and EU financial crime measures. Banks engage in customer due diligence, which always includes: (i) the identification and verification of a customer and/or beneficial owner and/or person acting on behalf of the customer; (ii) assessing, and where appropriate obtaining information on, the purpose and intended nature of the business relationship or occasional transaction; and (iii) conducting ongoing monitoring of the business relationship.”²⁸ International standards on customer due diligence and suspicious activity reporting have been established by the Basel Committee on Banking Supervision and the Financial Action Task Force (FATF).²⁹ Further, it is a key EU requirement for Member States to form specialised Financial Intelligence Units (FIUs) to gather, interrogate and share information between them that they receive, for example from financial institutions, to prevent, detect and disrupt money laundering and terrorist activity.

The network of FIUs and the sharing of information overcomes the fact that whilst information may have little or no value when handled in isolation, when it is brought together a fuller picture may well emerge. This information sharing approach has helped to identify and disrupt numerous organised crime and terrorist activities, and is viewed by international bodies such as FATF and Europol as being immediately valuable.³⁰ In the UK alone, the UK Financial Intelligence Unit (UKFIU) which sits within the National Crime Agency (NCA) received more than 634,000 Suspicious Activity Reports (SARs) during an 18 month period from October 2015 to March 2017 and analyses and distributes the intelligence gathered from these.³¹ SARs are used by a wide variety of law enforcement bodies in the UK and the EU to help investigate all levels and types of criminal activity; from international drug smuggling, human trafficking to terrorist financing and the movement of foreign fighters.³²

The timely sharing of cross-border information provides the most effective way to protect the financial system from money laundering and terrorist activity. Drawing on information and resource capabilities outside of a Member State ensures the most beneficial use of finite specialist resources.



25 See, United Nations Office on Drugs and Crime, Money Laundering and Globalisation, available at <https://www.unodc.org/unodc/en/money-laundering/globalization.html>

26 See, Europol, Money Laundering available at <https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/economic-crime/money-laundering>

27 See International Monetary Fund, Anti-Money Laundering/Combating the Financing of Terrorism – Topics, at <https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm>

28 See International Monetary Fund, Anti-Money Laundering/Combating the Financing of Terrorism – Topics, “Why is Customer Due Diligence necessary?” at <https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm>. The UK customer due diligence requirements are set out in the Money Laundering Regulations 2017, due to replace the Money Laundering Regulations 2007 on 26 June 2017. These implement the customer due diligence framework strengthened and expanded on by the Fourth EU Money Laundering Directive.

29 See Bank for International Settlements, Basel Committee On Banking Supervision, at <http://www.bis.org/bcbs/index.htm>; Financial Action Force, Latest News, at <http://www.fatf-gafi.org/>

30 See <http://www.fatf-gafi.org/media/fatf/documents/publicconsultation/Consultation-Guidance-Private-Sector-Information-Sharing-Jun17.docx> pp. 3-4.

31 See National Crime Agency, Suspicious Activity Reports (SARs) Annual Report 2017, p.6 at <http://www.nationalcrimeagency.gov.uk/publications/suspicious-activity-reports-sars/826-suspicious-activity-reports-annual-report-2017/file>

32 See National Crime Agency, UK Financial Intelligence Unit, at <http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/ukfiu>

Biomedical Research

Data is at the heart of biomedical research. Difficult medical questions can sometimes only feasibly be answered by undertaking complex research that requires collaboration between researchers, often in different countries. UK organisations involved in medical research benefit from being part of the EU's data protection regime, which allows data to flow between research institutions in the UK and the EEA.

Genomic research using longitudinal cohorts and medical bioinformatics studies generate vast amounts of rich data that contribute to UK, EU and global research initiatives. Biomedical research increasingly relies on international collaboration and sharing of data across borders, in order to:

- increase sample size and breadth, which is particularly important for research in rare diseases, as there may only be a handful of people with a condition in a single country;
- help ensure findings are generalisable across real populations; and
- allow patients to be identified for recruitment on clinical trials – multiple sites in different
- countries are often needed for clinical trials in order to include enough patients for the results to be statistically meaningful.

Data can be used in medical research to benefit patient health, through driving improvements in: understanding mechanisms of disease; diagnosis; patient safety; evaluating health policy; treatment and prevention; infection surveillance and service planning.³³

What types of data?

Data for medical research may contain among other things: clinical information about patients; biometrics; medical history; test results; genetic sequence information; genomic data; lifestyle questionnaire data; and family history information.

Genomic data is rich and unique to the individual and as such is considered a special category of personal data under the GDPR. While direct identifiers are removed from genomic data where possible, full genomic data sets may be considered personal data as they may still identify an individual. Nevertheless, these genomic data sets remain an important resource in medical research.

How data flows between the UK and EEA

Cross-border clinical trials require personal data to flow from clinical settings to a coordinating centre, often in another country. This enables the coordinating centre to identify potentially eligible participants for trials depending on factors such as their symptoms, severity, genetic test results and responsiveness to other treatments, as well as personal details like gender and age. Eligible participants can then be allocated to a trial arm and this information is sent back again to the relevant clinical team to enrol the patient into the trial.

Cross-country research projects and consortia often have data governance mechanisms, such as independent Data Access Committees to vet proposed research uses of data and their security and storage conditions. These enable researchers to apply for access to data, under the terms of a data access or material transfer agreement signed by the data controller and data user's respective institutions.

Difficult medical questions can sometimes only feasibly be answered by undertaking complex research that requires collaboration between researchers, often in different countries.

“Stable data transfer is crucial for all sectors – not just business. Crime doesn't respect national borders – so there are implications for national security and cross-border policing. Medical research communities operate on a global basis. And commerce does too – it's as easy to buy a book from an online shop based in Canada as it is to pop into a local bookshop here in Cambridge”

– Elizabeth Denham, UK Information Commissioner, Promoting privacy with innovation within the law, speaking at the Privacy Laws & Business Conference in Cambridge (4 July 2017), <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/promoting-privacy-with-innovation-within-the-law/>

33 The following input has been provided by The Wellcome Trust. See <https://wellcome.ac.uk/>

Case study: European Prospective Investigation into Cancer and Nutrition Study (EPIC)

The EPIC study has followed 521,000 participants in 10 European countries for 15 years to investigate the links between nutrition and cancer.³⁴ The size of the study means that it would not be possible for one country alone to coordinate and recruit enough people to generate robust results.

The study is coordinated by Imperial College, London, UK and the International Agency for Research on Cancer, Lyon, France and is funded by the World Health Organisation.

It has additional centres in France, the UK, the Netherlands, Sweden, Spain, Denmark, Germany, Greece, Italy and Norway.

Data is collected at the research centres, including Norfolk and Oxford and is stored at the data centre in France. The data collected and analysed has had direct impacts on public health policy, including WHO guidelines and UK Department of Health initiatives.

Case study: European Medical Information Framework (EMIF)

The EMIF project is developing common technical and governance solutions to improve access and use of health data across 14 countries, including the UK.³⁵ A common Information Framework (EMIF-Platform) will link up and facilitate access to medical and research data sources from participating countries for research into Alzheimer's disease and obesity.

The project will leverage data on around 40 million European adults and children by means of federating healthcare databases and cohorts from 6 different countries designed to be representative of the different types of existing data sources (population-based registries, hospital-based databases, cohorts, national registries, biobanks, etc.)

There are 12 UK partners involved in the project, including universities, SMEs and the pharmaceutical industry. It will be very challenging, if not impossible for UK institutions, organisations and businesses to continue to participate in this ground-breaking project without a viable means of sharing data with the EU. The result would be a reduction in the resources available for this vital work both in terms of funding and academic knowledge which will ultimately harm the progress of research across Europe.

Conclusion

The free flow of data is fundamental to the economic future and societal well-being of both the UK and the EEA. The next wave of UK and EEA economic growth, groundbreaking medical research and digital transformation will be powered by data. The free flow of data is also vitally important to fight international crime. As part of the UK's future relationship with the EU, a secure, robust and legal mechanism for data to flow freely as it does today must be found.

The next chapter of this report outlines the existing legal options that could be used to ensure data can continue to flow and the pros and cons of each. We conclude that adequacy is the best option to provide the legal certainty for businesses of every size and sector.

³⁴ See <http://epic.iarc.fr/>

³⁵ See <http://www.emif.eu/>

2 Ensuring the Free Flow of Data – What Options Exist?

Transfers of personal data among EEA countries are currently permitted under the European Data Protection Directive and that regime will continue under the new GDPR. However, both the Data Protection Directive and the incoming GDPR place restrictions on the transfer of personal data to third countries.³⁶

Leaving the EU and EEA will move the UK outside of the EU data protection framework making it a third country, as such, personal data will no longer be able to automatically flow between the UK and EEA countries without using approved legal mechanisms (or relying on derogations).

Transfers of personal data outside of the EEA to third countries are allowed under the GDPR so long as that data is afforded equivalent levels of protection as it would if it was located within the EEA. This is provided for in two ways:

- Through an assessment of the laws (and wider regulatory context) in the third country to which data is being moved which judges the country adequate to EU standards. This is known as adequacy.
- Through a series of derogations or alternative data transfer arrangements, described below, applied by companies and organisations moving personal data to countries outside of the EEA.

The UK Government has put forward a third option to allow for the continued flow of personal data in its proposal for the future data-sharing relationship between the UK and the EU. This option is outlined in the UK Government's future partnership paper the "Exchange and Protection of Personal Data" discussed later in Chapter 5.³⁷

This section will assess the current existing options for the cross-border transfer of personal data.

Mutual adequacy agreement between the UK and EU

Personal data may continue to move between the UK and EEA if an agreement of mutual adequacy is reached by the UK and EU.

An adequacy decision concerning a third country means that the third country is considered to provide essentially equivalent protection for personal data. Once a third country is determined adequate personal data may then be transferred from the determining territory to that country without the need to enter into any of the alternative data transfer arrangements (or rely on narrow derogations) outlined below. This provides assurances to governments, data protection authorities and citizens that their personal data will be protected effectively (and to a high standard) if it is transferred to that third country. This applies to all personal data transfers to recipients in the adequate third country, whether within the same business group or to external parties, and irrespective as to whether a recipient is a large multinational or an SME.

Once a third country is determined adequate personal data may then be transferred from the determining territory to that country without the need to enter into any of the alternative data transfer arrangements.

The difference between EEA and EFTA membership

In the event that the UK becomes a member of the EEA, the UK would not be a 'third country' for the purposes of the GDPR and therefore cross-border transfers of personal data among the UK and the other members of the EEA will be able to continue (subject to the remaining requirements of GDPR). As an important distinction, if the UK joins EFTA (a prerequisite to joining the EEA if a country is not an EU Member State), the UK will be a third country and will need to apply for adequacy for such period of time that it does not become a member of the EEA. The only EFTA state that has not joined the EEA is Switzerland, and Switzerland obtained an adequacy decision on 26 July 2000.

³⁶ See Chapter IV of the Data Protection Directive and Chapter V of GDPR

³⁷ See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

Adequacy has historically developed as an EU process, as outlined in the next chapter. However, the UK Government's Data Protection Bill, which forms part of the UK's implementation of GDPR, is expected to implement the same restrictions for the transfer of personal data outside the UK to third countries as exist in the EU.³⁸ This means that, unless amended, on exit from the EU the UK data protection regime will preserve the ability for the UK to determine a third country as adequate. The UK Government has indicated in its notes to the Data Protection Bill that the GDPR will be brought within the UK's domestic law following exit using the powers in the European Union (Withdrawal) Bill. Although not wholly clear at this stage, it is assumed that, in order for data to continue to flow from the UK to the EEA after exit, the UK would need to confirm that the EEA is an adequate destination for personal data transferred from the UK.

A mutual adequacy agreement between the UK and the EU would therefore automatically satisfy both data protection regimes while providing consistent, high standards of protection for personal data transferred between the UK and the EEA. This offers a significantly more efficient solution to ensuring that UK and EEA citizens can continue to benefit from the ability to move data between jurisdictions with a high level of assurance as to how their data will be handled in those locations. It also avoids the need for additional costs and resourcing (and operational uncertainty) for organisations and, critically, this solution is universal in application which means that all organisations and consumers benefit equally.

Therefore, to allow personal data to continue to flow between the UK and EEA as it does now, both the UK and the EU should reach an arrangement which finds each other's data protection regimes adequate. In this report this will be referred to as a mutual adequacy agreement and we will discuss both the process for how this can be achieved as well as connected considerations in the following chapters.

Alternative data transfer arrangements

In the absence of a mutual adequacy agreement, or in a scenario where the UK leaves the EU with no Brexit deal in place (that is, no Withdrawal Agreement and no Bilateral Agreement are in place), the established alternative legal bases for the transfer of personal data available at the business organisation level are:

- Binding Corporate Rules³⁹
- Standard Contractual Clauses⁴⁰
- Codes of Conduct⁴¹
- Certification⁴²
- Derogations⁴³

These alternative arrangements (other than the derogations from the GDPR requirements) are designed to help organisations by 'exporting' or imposing obligations that are substantially similar to European data protection law on the data recipients in the third country – the idea being that the alternative arrangements close any 'gaps' between the data protection and privacy laws of the third country and those of the EEA.

However, there are challenges, uncertainties, and disruptions associated with relying on such alternative arrangements for organisations in both the UK and the EEA, especially SMEs. Importantly they are not as wide ranging and accessible as an adequacy decision and they place ongoing and burdensome compliance obligations on individual companies.

The table below summarises the pros and cons of each alternative data transfer method and any role they could play to enable the continuous free flow of data once the UK leaves the EU. More detailed information on each alternative can be found in Annex 1.

Alternative Data Transfer Method	Pros	Cons	Significance for when the UK Leaves the EU
Binding Corporate Rules (BCRs)	<ul style="list-style-type: none"> • High watermark of data protection • Solves intra-group data transfers for large, complex multinationals • Can "live and breathe" with the multinational as its group expands 	<ul style="list-style-type: none"> • Generally only a solution for large multinational organisations and not SMEs • Lengthy and expensive process to obtain BCRs • Only a select few businesses currently have them • ICO's ability to act as lead authority likely to be lost following exit from the EU • Strictly, controller BCRs cannot be used for transfers between different groups of businesses 	<ul style="list-style-type: none"> • Those businesses with BCRs can use them to make data transfers into the UK lawful, but due to their cost and complexity, BCRs are not a viable solution for the great majority of companies • Certain vendors have sought processor BCR approval – this means that businesses, including SMEs, should be able to access the benefit of these processor BCRs under vendor terms and conditions/SLA

38 See <https://www.gov.uk/government/collections/data-protection-bill-2017>

39 See GDPR, Art. 47

40 See GDPR, Art. 46

41 See GDPR, Arts. 40 and 46

42 See GDPR, Arts. 42 and 46

43 See GDPR, Art. 49

Alternative data transfer method	Pros	Cons	Significance for when the UK leaves the EU
Standard Contractual Clauses (SCCs)	<ul style="list-style-type: none"> Commonly used and available data transfer solution Current pre-notification requirements required by certain Member States (for example Spain) will fall away under GDPR 	<ul style="list-style-type: none"> Difficult to address the realities of a network of cross-border data flows, require management and updating when flows change Can be expensive to put in place for multiple data flows Questionable as to whether they will in fact introduce additional data protection safeguards for transfers between the UK and EU, given the intended application of GDPR-standards in the UK Risk caused by ongoing case which has been referred to the European Court of Justice (CJEU)⁴⁴ and which is expected to rule on the validity of SCCs as a method for data transfer Likelihood that current SCCs will be replaced in the near future under GDPR; grandfathering process for existing SCCs unclear Do not suit certain processor flows that have a first transfer within EEA 	<ul style="list-style-type: none"> SCCs are likely to be the de facto fall-back solution in the absence of a UK adequacy decision The strength of UK data protection law both today and once GDPR has been implemented makes it questionable whether contractual obligations inherent in SCCs will provide additional safeguards for individuals or whether they will merely serve as contractual formalities Risk that SCCs will be put in place as at UK exit, but that they are not actively managed such that they become inaccurate as business' data flows change over time
Codes of Conduct	<ul style="list-style-type: none"> Opportunity for industry led standards Adherence can demonstrate good practice and encourage adoption within an industry sector 	<ul style="list-style-type: none"> Uncertain and lengthy approval process Does not solve data transfers for all industries Very unlikely to have a valid code of conduct finalised by all stakeholders by March 2019 Approach lends itself to being sector-specific only 	<ul style="list-style-type: none"> Codes of Conduct are an uncertain and lengthy process, and it is unlikely that any Code of Conduct will be approved in time for when the UK leaves the EU Further, any Code of Conduct will only address industry specific data transfers.
Certification	<ul style="list-style-type: none"> Opportunity for self-regulation Adherence can demonstrate good practice 	<ul style="list-style-type: none"> Uncertain and lengthy approval process No existing data protection accreditation bodies Requires renewal every three years Very unlikely to have a valid code of conduct by March 2019 Approach lends itself to being sector-specific only 	<ul style="list-style-type: none"> Similar to Codes of Conduct, certifications are unprecedented and carry uncertainty Certifications are unlikely to provide a solution for the UK and the EU within the needed timeframe
Derogations	<ul style="list-style-type: none"> As these are exceptions to the GDPR requirements, they do not require additional data transfer arrangements to be put in place 	<ul style="list-style-type: none"> Do not ensure that personal data is protected and safeguarded to EU high standards Can only be used in fact-specific and limited circumstances Not universal in application Do not provide a wide-ranging, continuing solution 	<ul style="list-style-type: none"> Derogations are fact-specific solutions and are generally unavailable (or will be difficult to rely upon with legal certainty) for the vast majority of cross-border data flows May be unsuitable for SMEs and other business models

44 See <http://www.europe-v-facebook.org/sh2/H CJ.pdf>

The processing of personal data for law enforcement purposes is provided for in the Data Protection Law Enforcement Directive. The UK's Data Protection Bill has introduced provisions to transpose this directive into UK law. In broad terms, transfers to a third country can only take place if necessary for law enforcement purposes and subject to various administrative requirements to be followed by the relevant agency or body. The regime provides that, in relation to cross-border transfers, in the absence of an adequacy decision, the transfers may only proceed where appropriate safeguards exist (such as the existence of a legally binding instrument) or a derogation is available.⁴⁵ Therefore, significantly, any mutual adequacy arrangement between UK and EU could also be a basis for the exchange of personal data for law enforcement purposes.

A mutual adequacy decision using the established GDPR adequacy process should be agreed between the UK and the EU, as soon as possible.

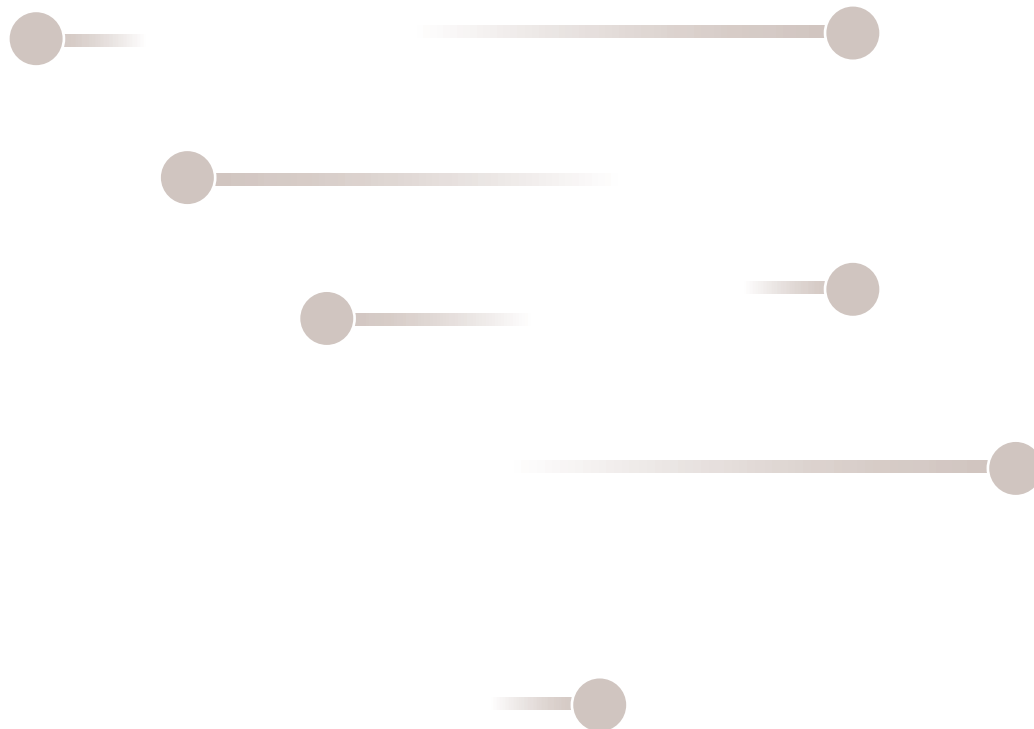
Conclusion

Once the UK has left the EU, it is clear that a secure and robust legal mechanism will be needed for the continued free flow of personal data between the UK and the EEA. Data transfer arrangements such as BCRs, SCCs, codes of conduct and certifications, and derogations, are precarious in terms of timing and viability and many are simply not relevant or suitable to SMEs and other business models. Also, for smaller businesses with less access to legal advice there is a real risk that alternative mechanisms may not be fully understood or will simply be overlooked, potentially leading to non-compliance with the GDPR and significant financial penalties of up to 4% of global annual turnover.⁴⁶

A mutual adequacy decision, based on existing adequacy processes in EU and UK data protection regulation would offer the most secure and robust legal basis for the future of UK-EU data flows if a more ambitious agreement cannot be reached. This is because it is an established and understood process.

A mutual adequacy decision would also facilitate the flow of personal data between UK and EEA agencies for law enforcement purposes.

In the next chapter, we set out the mechanics of an adequacy assessment and how they might be applied by the UK and EU, and the transitional arrangements that might be needed should it be impossible to complete an assessment before the withdrawal date.



⁴⁵ See Data Protection Law Enforcement Directive, Chapter V and Data Protection Bill, Chapter 3, Part 5

⁴⁶ See GDPR, Art 83. Infringements can amount to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

3 The Mechanics of the Existing Data Adequacy Process - How it Works

An adequacy assessment is the specific legal process by which the European Commission examines the essential equivalence of a third country's laws and practices. If the Commission accepts that the third country's laws offer the same level of protection as those of the EU then that third country is ruled to be adequate.

The main benefit of adequacy is that once a third country is determined to be adequate, personal data can be shared between that country and the EEA without firms in both jurisdictions needing to implement any of the alternative legal bases for data transfer discussed in the previous chapter. In addition, the thorough process of review involved in an adequacy ruling (outlined below) should help to ensure that the ruling can stand up to legal challenge.

The European Commission has already recognised Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay as providing adequate protection for personal data (in addition the European Commission has recognised the adequacy of protection of the EU-US Privacy Shield (discussed further below).⁴⁷

However, developments in data protection and privacy law have altered the concept of adequacy in recent years. As a result, there is a limited amount we can learn from prior adequacy decisions because these were made under the requirements of the 1995 Data Protection Directive (DPD) and related regulatory guidance and not under the new requirements of the GDPR.⁴⁸

If the UK seeks an adequacy decision, it will do so under the criteria established in the GDPR and based on a post-Schrems understanding of adequacy (for which see below). What this means is that any future adequacy assessment will not only evaluate a country's data protection and privacy laws, it will also examine domestic law more widely, as well as international commitments to determine whether there is a sufficient level of protection of fundamental rights and freedoms.

Specific factors include (without limitation) law enforcement's access to data and individuals' ability to seek judicial redress.⁴⁹

Developments in data protection and privacy law have altered the concept of adequacy in recent years.

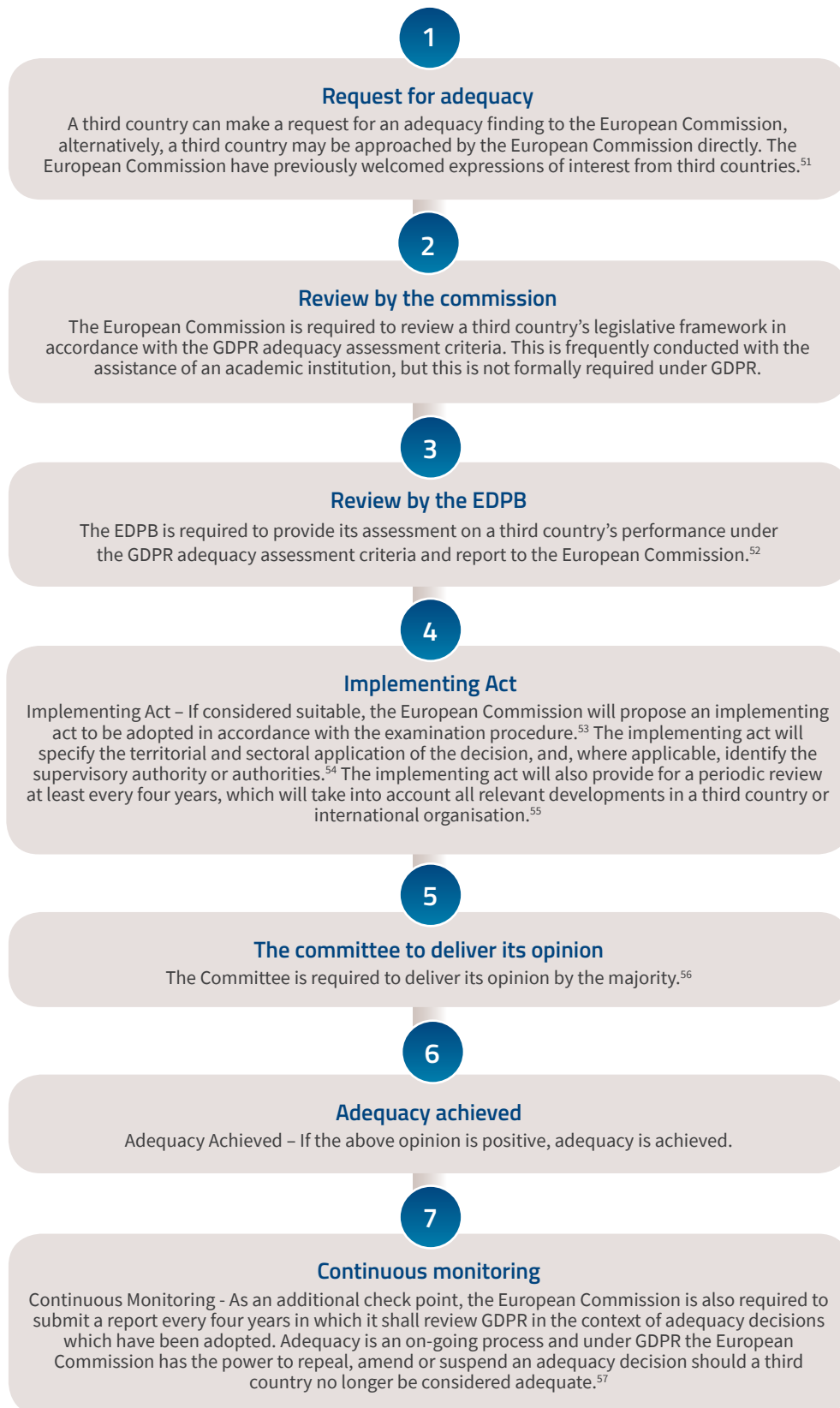
⁴⁷ See Commission decision on the adequacy of the protection of personal data in third countries available at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

⁴⁸ See European Commission, Working Party on the Protection of Individuals with regards to the Processing of Personal Data at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf; see also http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf.

⁴⁹ See GDPR, Art. 45(2)

The adequacy assessment process under the General Data Protection Regulation

Adequacy under the GDPR is a process involving several steps.⁵⁰ The specific process for obtaining an adequacy decision under the GDPR is as follows:



⁵⁰ This paper considers the process for full adequacy by a third country, as opposed to partial or sectoral adequacy.

⁵¹ See European Commission, Communication from the Commission to the European Parliament and the Council, January 2017, p.8 at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN>

⁵² See GDPR, Art. 70(1)(s)

⁵³ See GDPR, Art. 93(2)

⁵⁴ See GDPR, Art. 45(3)

⁵⁵ See GDPR, Art. 45(3)

⁵⁶ See Treaty on European Union available at http://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF, Article 16(4) and (5); and see Treaty on the Functioning of the European Union available at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT>, Article 238(3).

⁵⁷ See GDPR, Art. 45 (5)

A full, formal adequacy decision process will therefore involve the relevant third country, EU Member States, European Commission, European Data Protection Supervisor's Office and the Article 29 Working Party (soon to be the European Data Protection Board (EDPB)). In normal circumstances, an adequacy process can take between three to five years to complete.

How should the UK and EU secure mutual adequacy?

EU data protection law has been subject to multiple legal challenges over the past several years and any future data sharing relationship between the UK and the EU should be expected to receive significant levels of legal scrutiny by those concerned to ensure the maintenance of EU privacy standards.

Adequacy decisions are designed to ensure the highest level of legal certainty for organisations, institutions and public bodies relying on it as a legal basis for their transfers of data between jurisdictions. This is achieved not only by assessing the third-country's data protection regime in light of all circumstances surrounding data transfer, but also by relying on the processes set out in the GDPR and outlined above to demonstrate a robust examination and proper due diligence.

It is therefore important that any agreement between the UK and the EU evidences a detailed review of the respective legal frameworks and actions if it is to secure unhindered flows of personal data between the UK and EEA in a stable and legally robust way. By following the established GDPR adequacy process businesses and consumers in the UK and EU would have more assurance that the UK's adequacy decision is comprehensive and legally sound.

Timing concerns for the UK – EU future data sharing relationship

A full and formal adequacy decision could theoretically take effect immediately upon the UK leaving the EU. The GDPR anticipates that adequacy decisions be provided to third countries; it is silent as to which countries might be considered for adequacy and when. Although under the current legislative framework there is no provision for the European Commission to determine the adequacy of the UK as a third country while the UK remains a Member State, there is also no clear prohibition on doing so.⁵⁸ This offers an opportunity to forge new routes to adequacy.

Adequacy decisions are designed to ensure the highest level of legal certainty for organisations, institutions and public bodies relying on it as a legal basis for their transfers of data between jurisdictions.

Thus there would appear to be arguments allowing an adequacy assessment for the UK to begin now. As such, the European Commission can potentially begin an adequacy assessment of the UK immediately, despite the UK still being a Member State and not yet a third country. Alternatively, if the UK is not permitted to commence its formal adequacy application until the UK has left the EU and has become a third country, then UK and the EEA businesses, organisations and public bodies face a “cliff-edge” situation that requires alternative data transfer arrangements (which, as already demonstrated, are difficult and burdensome for many businesses) to be put in place with urgent effect.

However, even if the European Commission was to begin its adequacy assessment of the UK immediately, it is still unlikely that an agreement could be reached by the date of UK withdrawal. This is because a full, formal adequacy decision will require the involvement of relevant third countries, the EU Member States, the European Commission, the European Data Protection Supervisor's Office and A29WP (soon to be the European Data Protection Board). As discussed above, the formal adequacy process has historically taken three to five years with the quickest assessment completed in eighteen months.⁵⁹ Therefore the process of agreeing mutual adequacy should begin as soon as possible.

Although it is tempting to view the existing formal process of adequacy as something to be avoided due to the time involved and possible complications in the assessment of UK national laws on issues such as national security and surveillance, it is important to remember that this is the process prescribed by the GDPR and which would maximise the legal robustness of an adequacy decision for the UK as well as providing firms and organisations maximum certainty and reassurance. Moreover, carrying out such an assessment at this stage should be significantly more straight-forward as an administrative exercise because the UK is currently an EU Member State and, by virtue of the UK Data Protection Bill, is proposing to apply the GDPR after the UK's exit from the EU.

However, notwithstanding these considerations and given the urgent need for legal certainty, the desire to avoid burdensome and expensive alternative transfer mechanisms and the time it will take for a future data-sharing relationship to be agreed (regardless of whether it is mutual adequacy or a more ambitious arrangement), the UK and EEA should simultaneously consider mutual transitional arrangements. The possibility of a “cliff-edge” in March 2019 is a very real concern for businesses threatening confusion and significant costs as well as disruption for consumers and doubts for citizens over their data protection rights. Transitional arrangements which ensure that the transfer of personal data is not disrupted should thus be developed immediately and alongside any negotiations for a longer-term data-sharing / adequacy relationship.

⁵⁸ See Chapter IV of the Data Protection Directive; this would be the same under GDPR, Art. 45

⁵⁹ For Argentina

Transitional arrangements

To mitigate the risk to consumers and businesses that a long-term mutual adequacy decision or agreement will not be reached before the UK exits the EU, the negotiating parties should urgently prepare to implement transitional arrangements maintaining the status quo while the future data sharing relationship is negotiated.

Transitional arrangements will be required to avoid the risk of a regulatory “cliff-edge”. The sooner this parallel stream is progressed by the UK and the EU, the better the level of certainty will be for businesses – many of which operate with business change and procurement cycles of several months.

Any transitional arrangements must be based on the following principles:

- ensure the continued free flow of data between the UK and the EEA, as happens today;
- be time-limited with a mutual adequacy agreement in place once the transition period ends; and
- provide both sides with the ability to apply, conduct and proceed with the full adequacy process through to conclusion of a longer-term mutual adequacy arrangement.

Such transitional arrangements will offer the UK and the EU the time needed to conduct and conclude a future data-sharing relationship based on the existing adequacy model. The European Council has already indicated that it would be open to “transitional arrangements which are in the interest of the Union.”⁶⁰ In addition, the UK Prime Minister has stated in her Florence Speech that the UK recognises the need for transitional arrangements ‘for about two years’. The time limited nature of any transition underscores the fact that, while the UK and the EU might have a reasonable amount of time to pursue a long-term data-sharing relationship, any solution must begin in tandem along with the planning for a transitional arrangement.

Although the details may take time to negotiate, it will be critical that UK and EU businesses are given early sight and awareness of any possible transitional arrangement. This is because business procurement and planning cycles can have significant lead-in times, and, without early visibility of possible transitional adequacy arrangements, businesses will need to incur costs implementing fall-back data transfer solutions or, potentially, take alternative investment decisions.

Conclusion

Adequacy is a complex and comprehensive process that in any ordinary circumstance takes time to complete - the unique legislative and political challenges posed by the UK’s withdrawal from the EU are likely to only make the process more complicated. Therefore, negotiations should begin immediately over a future data-sharing relationship between the UK and EU based on the adequacy model in the GDPR. This is true whether a bespoke model or the adequacy process given in the GDPR is followed.

If mutual adequacy decisions cannot be reached before the UK’s withdrawal, transitional arrangements will be needed within the Withdrawal Agreement in order to avoid a “cliff-edge” that harms the millions of consumers and thousands of businesses which rely on the ability to transfer data between the UK and EEA. Because of the danger a “cliff-edge” poses to businesses and consumers, the UK and EU Governments should begin making plans for transition arrangements in parallel to the negotiations over the future relationship and based on the principles set out above.

The following chapters consider the implications of the adequacy process under the GDPR, and what this means for the roadmap for achieving a relationship based on adequacy between the UK and the EU. We will also set out arguments which may be raised in anticipation of any potential challenges inherent in the data protection regimes of the UK and the EU.

It will be critical that UK and EU businesses are given early sight and awareness of any possible transitional arrangement.

60 See European Council guidelines for Brexit negotiations available at <http://www.consilium.europa.eu/en/press/press-releases/2017/04/29-euco-brex-it-guidelines>

4 Roadmap for UK – EU Adequacy

There may be a number of perceived barriers to the UK and EU reaching an agreement based on the existing GDPR adequacy model. In this chapter, we look at the challenges to an agreement based on adequacy and make recommendations for how these can be overcome. Similar challenges have been overcome before, as was demonstrated with the EU-US Privacy Shield negotiations.

Economic and political factors that support a mutual UK – EU adequacy decision

The European Commission has publicly acknowledged the benefits of adequacy for third countries and the EU, in particular, the “opening up [of] commercial channels for EU operators,”⁶¹ and the “new opportunities, notably through adequacy findings, to further facilitate data flows while guaranteeing the continued high level of protection for personal data.”⁶² This suggests not only the economic, but also the political benefits to the EU of maintaining the UK within a GDPR framework for data protection.

Past adequacy decisions have been impacted by political and economic factors as much as legal considerations. It is likely that moving forward this will not change; the European Commission has recognised the following criteria used to determine which third countries should be considered adequacy candidates.⁶³

It is recognised that there is a strong alignment between the EU and the UK’s data protection frameworks. This is true not just of their legal regimes, but of the shared values and objectives at the international level which underpin them. This is especially notable in the shared desire for high data protection standards. By embracing the data-driven revolution Europe, including the UK, has positioned itself as a global leader in the development of data protection and privacy regulations and standards with current European data protection laws being used as the blueprint for many other countries internationally. This common focus on strong data protection for citizens can form the basis for continued collaboration. If found to be adequate and retained in the fold of EU data protection, the UK and the EU could continue to work together on common data standards, particularly with regards to the propagation of international/multilateral data regulation best practice. As a source of further strength, for transfers to third countries it could prove possible to closely align or, potentially, mutually recognise UK and EU adequacy decisions.

European Commission Third Country Candidate Criteria (January 2017)

- **Commercial relations** - the extent of the EU’s (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;
- **Scale of data flows** - the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;
- **Role model status to third countries** - the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and
- **Political relationship** - the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.

61 See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, p.6 at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN>

62 See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, p.7 at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN>

63 See https://ec.europa.eu/newsroom/document.cfm?doc_id=41157

Furthermore, any failure for the EU and UK to agree adequacy could cast doubts over the viability, effectiveness and purpose of the EU's adequacy process. This is all the more important given the EU's adequacy decisions underway or soon to commence with Japan and South Korea (and possibly India and Mercosur countries in the near term).⁶⁴ This is in addition to the imminent review of the status of third countries with existing adequacy findings such as Canada and Switzerland which need to be updated to reflect GDPR. In this context, a failure by the UK to receive an adequacy decision from the EU, even with a GDPR-based UK data protection regime, may be a reason for grave concern for other countries seeking data transfer agreements with the EU. This could cause a delay or even a reluctance on the part of other third countries to explore a GDPR-based adequacy path with the EU.

Assessing the UK's position for achieving an adequacy decision

How has the adequacy process changed over time?

When assessing the UK's position for achieving an adequacy decision, it must first be remembered that the adequacy criteria has developed over time. As has been well documented, a recent legal case brought by Maximillian Schrems against the Irish Data Protection Commissioner challenged the protection of personal data shared under the EU/US Safe Harbor Framework.

As a result of the Schrems decision, the European Commission will review, and take into account, other domestic legislation which impacts on a third country's data protection framework (as well as the wider regulatory context) as part of the adequacy process. This means that the adequacy assessment will not only examine the third country's data protection legal regime but will consider the entirety of the third country's domestic law and binding international commitments that relate to the processing of personal data.

Case Note: Maximillian Schrems v Data Protection Commissioner

In October 2013, the CJEU reviewed the validity of the EU/US Safe Harbor Framework – a partial European Commission adequacy decision. The Safe Harbour Framework permitted US organisations to voluntarily self-certify to a set of data protection principles that were analogous to requirements under European data protection law.⁶⁵ By doing so, those organisations were deemed to be an adequate destination for personal data.

In its judgment, the CJEU reviewed the requirements that the European Commission must consider when determining the adequacy of a third country. In particular, the CJEU considered the requirement to assess adequacy in light of all the circumstances surrounding a data transfer operation.⁶⁶

The CJEU held that the term “adequate level of protection,” must be understood as requiring the third country “to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union”, including those rights and freedoms guaranteed within the Charter of Fundamental Rights, including Article 7 (respect for private and family life) and Article 8 (right to data protection). In summary,⁶⁷ the CJEU highlighted the following factors to be reviewed as part of any adequacy assessment:

- Domestic legislation to protect personal information;
- Compliance with the EU data protection principles;
- Independent regulatory supervision;
- Enforcement abilities of the competent regulator;
- Judicial remedies;
- Rule of law;
- International commitments a third country has entered in to, in particular in relation to the protection of personal data; and
- Interference with the right to privacy.

Ultimately, the CJEU found that the European Commission's decision implementing Safe Harbor considered the adequacy of the Safe Harbor principles and the implementing FAQs. However, significantly, the Commission had failed to consider the wider US legislation which impacted on data privacy, such as legislation which requires data collection for US national security purposes. Consequently, the CJEU held that the Safe Harbor Framework was invalid due to deficiencies in the European Commission's adequacy assessment process.⁶⁸

Following this ruling, negotiations between the EU and US led to the conclusion of the EU-US Privacy Shield adequacy decision in 2016, which replaced the Safe Harbor Framework.⁶⁹

⁶⁴ See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, p.8 at <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN>

⁶⁵ See Decision 2000/520/EC approved by the Commission on 26 July 2000

⁶⁶ See Data Protection Directive, Art. 25(2)

⁶⁷ See Case C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner (para 73)

⁶⁸ See Case C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner (para 98)

⁶⁹ See http://europa.eu/rapid/press-release_MEMO-16-434_en.htm

Elements of GDPR adequacy assessment

Given that the GDPR does not come into legal effect in Member States until 25 May 2018 and that therefore no adequacy decision under GDPR has been made, there is some ambiguity as to what criteria a GDPR adequacy assessment might include. However, based on an analysis of recent Article 29 Working Party (A29WP) guidance, CJEU case-law and European Commission communications, it may include some or all of the following criteria:⁷⁰

- Domestic legislation to protect personal information
- Compliance with the EU's data protection principles
- Systematic use of the highest level of protection for sensitive personal data
- Independent regulatory supervision
- Enforcement powers of the regulator
- Judicial remedies
- Case law and application
- Transparency for individuals as to their judicial rights
- Derogations for national security purposes
- Derogations by public authorities
- Derogations for defence purposes
- Derogations for crime prevention purposes
- Rule of law
- Membership of European Convention for Human Rights
- Signatory to Convention 108⁷¹
- Onward transfer principles
- International commitments a third country has entered in to, in particular in relation to the protection of personal data
- Interference with the rights to Data Protection/Privacy

In addition, the recent opinion of the CJEU on the compatibility of the EU-Canada Agreement on transferring passenger information in the fight against terrorism with the EU Treaties and Charter of Fundamental Rights will also be instructive. The opinion highlights the requirements for the transfer of information to be compatible with the Charter of Fundamental Rights in that context.⁷²

UK's arguments for adequacy

There are a number of factors which support an argument for UK adequacy under GDPR. These include the facts that the UK has implemented the current EU Data Protection Directive, it will implement the forthcoming GDPR into domestic law through the European Union (Withdrawal Bill) and it is legislating for GDPR derogations and data processing not covered by the GDPR through the Data Protection Bill. The Data Protection Bill also proposes that national security/intelligence services are required to comply with internationally recognised data protection standards based on Council of Europe Data Protection Convention 108. Finally, the UK has an experienced and proactive data protection authority (the ICO) with a range of sanctions and powers (together with a strong regional structure).

Furthermore, in liaising informally with European DPAs, it is clear that a key concern was whether the UK would retain the GDPR once the UK has left the EU. The UK Government has signalled a clear and positive intention to do so.⁷³ Further, in a recent position paper published on 6 September 2017 the European Commission has outlined its requirements in order for UK businesses to continue to hold the personal data of EEA citizens that was transferred before the UK's exit.⁷⁴ That report suggests that the implementation of GDPR by the UK would remove the need for UK organisations to delete relevant personal data (therefore suggesting an expectation that the UK's data protection regime will be sufficiently robust following the implementation of GDPR).

However, an issue the UK Government may wish to consider is retaining Articles 7 and 8 of the Charter of Fundamental Rights, which provides rights to privacy and to data protection, as an indication that the UK is committed to data protection as a fundamental right. In Schrems, as elaborated upon by the European Commission, it is clear that the laws of the third country do not need to identically replicate EU data protection law, but that they must nonetheless deliver a high level of protection.⁷⁵

What is clear is that any UK adequacy determination will need to consider the totality of UK law and the wider regulatory context, and not just UK data protection and privacy law – meaning those areas of UK law (for example, national security) which were previously outside the scope of EU competence and review, together with the extent of the UK's derogation from the GDPR, are now in scope in terms of an adequacy determination.⁷⁶

⁷⁰ See GDPR, Art. 45(2)

⁷¹ See GDPR, recital 105

⁷² See Opinion 1/15 EU/Canada PNR Agreement, 26th July 2017 <http://curia.europa.eu/juris/document/document.jsf?text=&docid=193216&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1130149>

⁷³ See <https://www.gov.uk/government/speeches/queens-speech-2017>

⁷⁴ https://ec.europa.eu/commission/sites/beta-political/files/use-data-protection-information_en.pdf

⁷⁵ See Case C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015, Maximilian Schrems v Data Protection Commissioner (para 73)

⁷⁶ See TFEU, Art. 72

“The adequacy standard does not require a point-to-point replication of EU rules. Rather, the test lies in whether, through the substance of privacy rights and their effective implementation, enforceability and supervision, the foreign system concerned as a whole delivers the required high level of protection. As the adequacy decisions adopted so far show, it is possible for the Commission to recognise a diverse range of privacy systems, representing different legal traditions, as being adequate.”

- COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Exchanging and Protecting Personal Data in a Globalised World⁷⁷

Addressing areas of concern for UK adequacy

Following the Schrems decision (and several CJEU decisions, such as *Tele2 Sverige* and *Watson* (judgment on 21 December 2016)), some concern has been expressed over whether powers granted to UK authorities pursuant to the Investigatory Powers Act 2016 and the Digital Economy Act 2017 bring into question whether UK law is consistent with GDPR and, most importantly, meets the adequacy standard of essential equivalence on its own.⁷⁸ These concerns are well known and citizens rights in this regard must be taken seriously. There are a number of ways that these concerns could be addressed.

Through the implementation of the Data Protection Bill the UK government is making it clear that the UK will continue to have a strong data protection standard for its citizens and the citizens of other countries whose data is processed in the UK. The UK Government announced plans, as part of the Data Protection Bill, to “legislate to provide for a distinct data protection framework for national security purposes, one that builds on and modernises, the existing regime” and which will be based upon the Council of Europe Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (Convention 108).⁷⁹

Further, the safeguards inherent in the Investigatory Powers Act 2016 and the Digital Economy Act 2017, when assessed in light of the UK Human Rights Act 1998, may support its arguments for a finding of adequacy as they address some of the same concerns that were raised in the Schrems judgement and addressed through the EU-US privacy Shield arrangement. For example, in respect of the Investigatory Powers Act 2016, the redress mechanisms available for individuals; the role of the Judicial Commissioner as part of the Act’s “double-lock”; the role of various of Codes of Practice; and oversight offered by the Investigatory Powers Commissioner (IPC), the ICO and the Investigatory Powers Tribunal.

Furthermore, section 2 of the IP Act acknowledges that the requirements of the Human Rights Act 1998 (and thereby the ECHR) may be taken into account when relevant decisions are undertaken. Indeed, the Rt Hon Matthew Hancock MP, UK Minister of State for Digital, recently stated “the activities of UK security and intelligence agencies are governed by one of the world’s most robust legal frameworks and oversight arrangements, which ensure UK intelligence activity adheres to strict principles of necessity and proportionality.”⁸⁰

However there is a risk that these arguments may not be determinative. To enhance its case for adequacy, the UK Government should consider all relevant legislation which may be perceived to interfere with a favourable adequacy finding to satisfy itself that such laws are consistent with the GDPR generally and that any additional safeguards that may be necessary are put in place.

For example, but without limitation, the UK Government could consider producing a statement as to its interpretation of how the Investigatory Powers Act 2016 and Digital Economy Act 2017 would help the UK to meet the essential equivalence test. Any such statement could emphasise for example:

- the redress mechanisms available for individuals, with particular regard to the respective roles of the Investigatory Powers Commissioner, the ICO, and the Investigatory Powers Tribunal; and
- the rights of individuals under UK GDPR and the protections potentially offered by the Human Rights Act 1998.

Additionally, there may be an opportunity for the UK government to offer further protections by building in further privacy-related checks and controls in updated IPA 2016 Codes of Practice.

Finally, similar to EU concerns over ancillary UK laws which impact personal data and individual privacy, there may be concern that once the UK leaves the EU, it will no longer be party to the EU-US Umbrella Agreement – the agreement between the EU and the US which regulates the transfer of personal data for criminal law enforcement purposes. In fact, the UK may need to enter into a similar agreement with the US to help preserve the argument that the totality of the UK’s domestic laws and international agreements are essentially equivalent to the EU (discussed further in chapter 6). Further, the UK would need to be designated a “covered country” under the Judicial Redress Act, in order to ensure that EU individuals can seek recourse under the U.S. Privacy Act 1974 if their personal data is transferred to the US through the UK. The UK Government should begin talks with the US Government now to address these issues to best avoid disruption to a future UK adequacy arrangement with the EU.

⁷⁷ See Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, available at https://ec.europa.eu/newsroom/document.cfm?doc_id=41157

⁷⁸ For example, there are a number of ongoing court cases relating to the UK’s surveillance laws, including a case before the European Court of Human Rights, expected to report in early 2018.

⁷⁹ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf

⁸⁰ Letter to Lord Boswell of Aynhothe, Chairman of the European Union Committee in the House of Lords, see <http://www.parliament.uk/documents/lords-committees/eu-home-affairs-subcommittee/data-protection-report-response.pdf>

Given the tensions and concern in respect of surveillance and national security processing there is merit in considering additional potential measures that have been used in other data transfer agreements and could be applied ahead of any adequacy assessment. Similar concerns were seen in the negotiation of the EU-US Privacy Shield Framework introduced following the Schrems ruling. Although the US does not have a comparable legal framework in respect to data protection these considerations may nonetheless provide helpful context and reference points for the UK and EU.

Closer Look – EU/US Privacy Shield Framework

Following the invalidation of the EU/US Safe Harbor Framework in Schrems, the European Commission considered not only the data protection principles, but also the totality of US law and determined that the US Government needed to make additional commitments in order for the EU-US Privacy Shield Framework to meet the essential equivalence test under Schrems, including:

Purpose limitation to the bulk collection of data for national security purposes

Under Presidential Policy Directive 28 (PPD-28), the US committed to only collect bulk signal intelligence for six specific purposes: (i) detecting and countering certain activities of foreign powers; (ii) counterterrorism, (iii) counter-proliferation; (iv) cyber-security, (v) detecting and countering threats to US or allied armed forces, (vi) and combating transnational criminal threats including sanctions evasion.⁸¹

Creation of an independent ombudsperson

The US designated a government official who is independent from the intelligence community (currently the Under Secretary of State for Economic Growth, Energy, and the Environment) to act as Ombudsperson to the EU/US Privacy Shield Framework – thus creating a point of contact for EU governments to raise concerns regarding signals intelligence activities conducted by the United States.⁸²

Additional redress mechanisms

The EU-US Privacy Shield Framework offers an enhanced redress mechanism via the Judicial Redress Act that allows EU individuals to (i) complain directly to the company; (ii) seek alternative dispute resolution; (iii) complain to a European DPA; (iv) complain to a US regulator (e.g., Department of Commerce and the Federal Trade Commission); and (v) if the complaint is not fully resolved after using the earlier mechanisms, seek recourse under the Privacy Shield Arbitration Panel.⁸³

Annual review and suspension

There is a provision for the annual joint review of the EU/US Privacy Shield Framework, and a related suspension clause. The first annual review was conducted by the European Commission in September 2017 and reported in October 2017. The review found that, while improvements could be made to the practical implementation of the Privacy Shield, “the Commission concludes that the United States continues to ensure an adequate level of protection for personal data transferred under the Privacy Shield from the Union to organisations in the United States.”⁸⁴ The Privacy Shield is therefore currently maintained as a mechanism to transfer personal data between the EU and US.

Conclusion

Following many years of integration of data protection law, both former and upcoming, and the strong role played by the UK's ICO in developing data protection policy and best practice, the UK is better positioned than any other country to be considered an adequate destination for the transfer of personal data from the EEA. This chapter has set out the factors that will need to be considered for the UK to obtain a formal adequacy decision from the European Commission taking account of both the Schrems decision and the entry into force of the GDPR. If a more ambitious future data-sharing relationship is pursued, it will be based on the adequacy model and many considerations will remain pertinent.

Whichever model is pursued, timing will be a key factor. The priority should be to avoid a “cliff-edge” that would be harmful to the millions of consumers who rely on the ability of many thousands of businesses and other organisations to transfer data between the UK and the EEA. Therefore, as the future relationship is negotiated, any residual concerns which could delay or hamper an agreement should be addressed immediately starting with the mechanisms given above.

Even with these steps, a transitional arrangement for data will be necessary in order to avoid a “cliff-edge”. Discussions should take place as soon as possible, to determine what those transitional arrangements would look like, and they should be open and transparent so that industry has the certainty it needs.

⁸¹ See <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities>

⁸² See <https://www.state.gov/e/privacyshield/ombud/>

⁸³ See http://ec.europa.eu/justice/data-protection/files/eu-us_privacy_shield_guide_en.pdf

⁸⁴ See http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619

5 UK Government Proposal for the Exchange and Protection of Personal Data - August 2017

On 24 August 2017 the UK Government published 'The exchange and protection of personal data: A future partnership paper.'⁸⁵ This paper envisages a bespoke and untested model for data flows between the UK and EU post-Brexit, 'building on the existing adequacy process', and would seek to maintain a role for the UK Information Commissioner's Office at the European level.

The position paper clearly recognises the importance of maintaining the free flow of personal data between the UK and EU after the UK's withdrawal. Industry welcomes the fact that the UK Government has raised this issue to the top of the negotiation agenda and urges both sides to de-politicise this topic in order to avoid disruption.

The UK Government appears to suggest that a mutual recognition agreement based on the usual adequacy principles would be sought as part of the Brexit Withdrawal Agreement. The agreement would then be replicated into a new and bespoke bi-lateral agreement between the UK and EU once the UK is officially a third country.⁸⁶ This would have the benefit of ensuring that data can continue to flow from the moment the UK is no longer a member of the EU, which is a fundamental imperative.

A welcome proposal in the UK Government's paper is that of maintaining a prominent role for the UK ICO at the European level.⁸⁷ The benefits of continued close regulatory cooperation are significant for both sides: continued exchange of regulatory expertise, thought leadership and regulatory innovation. It would also provide safeguards against risks of duplicative regulatory oversight and ensure consistent application of privacy rights and data protection standards across the EEA and the UK.

However, there are still gaps when it comes to the UK's current position. For instance, there is no discussion for how a future data-flow relationship with the EU would impact upon data transfers between the UK and the US, which is another crucial partner for both the UK and the EU (or, indeed, with other important non-EU countries). There is also a lack of clarity on how to address and overcome potential stumbling blocks which could arise while negotiating such an agreement, including the issue of UK national surveillance laws, which was discussed in the preceding chapter of this report.

Nor is there any detail provided on the legal basis of any such agreements with the EU and therefore the level of legal certainty that this bespoke arrangement would provide to businesses when considering their future operational decisions. Such an arrangement has not been agreed before and it is not entirely clear on what legal basis it would be established, the timing involved in taking this approach, or the risk that political factors could undermine this approach resulting in a "cliff-edge" outcome. As no Member State has previously left the EU and sought to agree mutual recognition/adequacy while remaining a Member State, there is no precedent as to what a Withdrawal Agreement can contain and how it may impact pre-existing Primary and Secondary EU law.⁸⁸

The benefits of continued close regulatory cooperation are significant for both sides: continued exchange of regulatory expertise, thought leadership and regulatory innovation.

⁸⁵ See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

⁸⁶ See paras 29 and 30 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

⁸⁷ See also section 118 of the Data Protection Bill. A proactive, international role is clearly anticipated for the ICO.

⁸⁸ See <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:l14534>

Qualified Majority voting is the procedure used for the Withdrawal Agreement, and it is part of the ordinary legislative procedure (also known as the co-decision procedure) – thus subjecting the Withdrawal Agreement to review by the European Parliament along with its related political exigencies.⁸⁹

If the UK and EU wish to include a data flow arrangement in the Brexit Withdrawal Agreement they must therefore consider the pace of wider Brexit negotiations and the various other factors at play; given the need for longer-term planning, and the length of procurement cycles, businesses will not be able to react in time should any agreement fall away at the last moment due to political differences.

The European Commission have yet to respond to the UK Government's position paper at the time writing. On 7 September 2017 the Commission published a paper with the subject 'Position paper transmitted to the EU27 on the Use of Data and Protection of Information Obtained or Processed before Withdrawal Date'.⁹⁰ However this paper principally addresses issues in relation to data obtained or processed up until the moment the UK withdraws from the EU, and does not address any aspect of the future relationship. Without agreement from the European Commission to begin talks on the UK Government's proposal, there is concern that there simply will not be sufficient time left to agree such a relationship as part of the withdrawal talks.

Conclusion

The UK Government's position paper on a future relationship between the UK and EU on data flows provides a starting point for discussion and presents certain advantages, such as: mutual adequacy arrangements to provide for the free flow of personal data; and a continued role for the ICO at European level. These aims and objectives are welcomed by industry.

If the UK Government's position were to be realised it would be welcomed. However, more detail is needed as to how this proposal would work in practice and what process would be followed to achieve it. Specifically, more detail is needed on the important issues of legal clarity, certainty, timing and political risk given the important decisions at stake and the timeframes in which businesses are operating. A detailed reaction to the UK's opening negotiation position from the EU is also required.

If the UK and EU wish to include a data flow arrangement in the Brexit Withdrawal Agreement they must therefore consider the pace of wider Brexit negotiations and the various other factors at play.



⁸⁹ See TFEU, Art. 283; see also <http://www.consilium.europa.eu/en/council-eu/voting-system/qualified-majority/>

⁹⁰ See https://ec.europa.eu/commission/sites/beta-political/files/use-data-protection-information_en.pdf

6 Onward Transfers from the UK and their Impact on Adequacy

International transfers and onward transfers

A key characteristic of the forthcoming GDPR is its extraterritorial reach. The GDPR is designed not only to ensure the protection of EEA citizens' personal data within the EEA, but also when it is transferred onwards overseas. Under the GDPR the process for controlling for the transfer of personal data from one third country to another is known as "onward transfer".⁹¹

Key Concepts

Onward transfer

Data transfer restrictions exist to ensure that adequate protections and safeguards follow personal data as it moves from country to country. Each time data jumps to a new country, it has been transferred, and "onward transfer" refers to all subsequent transfers after the initial transfer:



As the UK establishes its own data protection regime, it will be necessary to include frameworks and restrictions for the sharing of data with third countries. A UK international and onward transfer regime following the UK's exit from the EU is necessary for three reasons:

- having a comparable international and onward transfer regime will facilitate the UK's assessment of EEA adequacy under UK data protection law after exit;
- the EU requires evidence of regulation of onward transfers of its own citizen's personal data to GDPR standards in order to find the UK adequate; and
- the UK must regulate international and onward transfers of personal data leaving the UK to satisfy EU and UK data protection law requirements in any event.

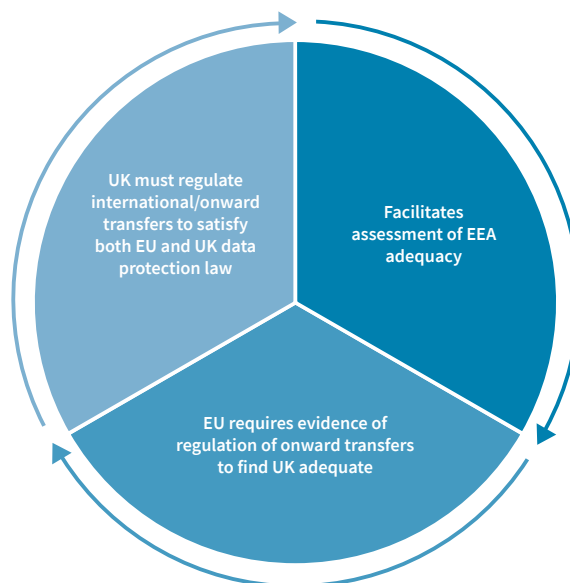


Figure 1: International and onward transfers: necessity for UK regime

91 See GDPR Art 44

Currently, the UK defers entirely to the EU on matters of adequacy decisions as a consequence of the application of GDPR and the UK remaining a Member State until March 2019. After the UK leaves the EU it will have the option of replicating the international and onward transfer model set out in the GDPR (which the UK helped to draft) in respect of transfers of personal data from the UK. The advantages of using this model are given below:

The UK implements a GDPR-based transfer regime	UK: Advantages	EEA: Advantages
<p>The UK maintains its current data transfer regime based on adequacy decisions and alternative data transfer solutions/derogations.</p> <p>The UK can facilitate continued harmonisation of strong data protection standards by taking the same view on adequacy decisions as the EU and by making use of EU's forthcoming revision to SCCs.⁹²</p> <p>The UK would enter into its own Privacy Shield Framework with the US and other bilateral data transfer agreements, as it has committed to do.⁹³</p>	<ul style="list-style-type: none"> • Leveraging of adequacy assessments by the EU. • Improves UK-EU relations in regard to privacy best practice, and wider afield. • Continues the current legal data protection regime ensuring stability. • Avoids balkanisation of alternative data transfer solutions and allows the UK to make use of existing mechanisms. • EEA and UK common pressure/leverage over third countries. 	<ul style="list-style-type: none"> • Similar to EU regime. • Improves UK-EU relations in relation to privacy best practice, and wider afield. • Reinforces EU promotion of GDPR as de facto global privacy standard. • EEA and UK common pressure / leverage over third countries (eg US in respect of the Privacy Shield Framework). • Continues the current legal data protection regime ensuring stability.

Transfer to third countries

In regard to the EU, at the same time that the EU's UK assessment begins to take place, the UK should conduct a similar assessment of the EEA. The UK's involvement in the creation of the GDPR and its intimate familiarity with European data protection law should facilitate a relatively quick assessment process. Nevertheless, in order to ensure that measures are in place by the date of the UK's exit the ICO and the UK government should begin preparations now such that it is in a position to issue an EEA adequacy decision under the UK's domestic data protection law following exit from the EU.

On exit from the EU, the UK will likely need to enter into an agreement with the US that is substantially similar to the EU-US Privacy Shield Framework.

In addition, the UK has also said that it will "liaise with those third countries to ensure that existing arrangements will be transitioned over at the point of exit".⁹⁴ Those third countries are the countries that are currently adequate locations for the transfer of data from the UK by virtue of the current adequacy decisions under EU data protection law. The most important of these is the US, which is able to receive personal data from the EEA through the EU-US Privacy Shield Framework agreed in 2016.

Therefore, on exit from the EU, the UK will likely need to enter into an agreement with the US that is substantially similar to the EU-US Privacy Shield Framework. This will be necessary to ensure the highest levels of protection for both UK and EEA citizens' data, as is their right. Switzerland is the most comparable example as it has a separate Swiss-US Privacy Shield agreement. It took an additional seven months after the US-EU agreement for Switzerland and the United States to reach political agreement. We thus recommend that the UK and the US begin working now on a UK-US Privacy Shield Framework to avoid any disruption to the cross-border data flows once the UK leaves the EU (and to offer an additional option for compliant onward transfers of personal data received in the UK from the EEA). We outline the necessary steps on the next page:

⁹² See <https://www.edoeb.admin.ch/datenschutz/00626/00753/index.html?lang=en>

⁹³ See UK Government Exchange and Protection of Personal Data, para 31 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

⁹⁴ See UK Government Exchange and Protection of Personal Data, para 31 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

Required Steps for a UK/US Privacy Shield Framework

- 1. Commence Project** – The UK and US government will need to initiate talks on a possible UK-US Privacy Shield Framework. Participants in this initial meeting should likely include the representatives from the UK's ICO and the US Department of Commerce, Federal Trade Commission (FTC), Department of Transportation (DoT), and State Department. As there is already a Memorandum of Understanding between the ICO and the FTC, there very likely already exist a strong collaborative relationship between the UK and the US which can be leveraged.⁹⁵
- 2. Umbrella Agreement and Judicial Redress Act** – Fundamental to the EU/US Privacy Shield Framework are the enhanced redress rights afforded by the US Government to EU individuals under the Umbrella Agreement and the Judicial Redress Act.⁹⁶ Upon leaving the EU, the UK will need to enter into an agreement similar to the Umbrella Agreement with the US if the UK is going to continue to take the benefits of the Umbrella Agreement. Similarly, the US Attorney General will need to designate the UK as a “covered country” under the Judicial Redress Act for both EU and UK individuals to be afforded rights under the US Privacy Act 1974⁹⁷ if their personal data is to be transferred to the US from the UK.
- 3. Political Agreement** – The UK and the US will need to reach political agreement on the content of the UK-US Privacy Shield Framework. As the EU-US and Swiss-US Privacy Shield Frameworks are already in place, they should provide the foundation for a UK-US Privacy Shield Framework.⁹⁸
- 4. National Implementations** – Both the UK and the US will need to implement a UK-US Privacy Shield Framework into their local legal frameworks:
 - a. **UK** – The UK will need to follow the procedures in its domestic data protection legislation following its exit from the EU to designate the US as an adequate destination for personal data.
 - b. **US** – The US executive agencies administering and enforcing the Privacy Shield Framework will need to commit to extending the Privacy Shield Framework to the UK. When this was done for Switzerland, letters from the US FTC, DoT, and Department of State were sent to Switzerland as evidence of these commitments.⁹⁹ In addition, letters from the US Office of the Director of National Intelligence and the Department of Justice were also sent as assurances in regard to US national security, law enforcement, and public interest purposes for processing personal data.
- 5. Entry into Force** – The UK and the US will need to agree a date from which the US will begin accepting applications from US companies to participate in the UK-US Privacy Shield Framework.

Conclusion

Onward transfer is a key consideration for both the UK and EU as they look to ensure that their citizens' rights receive high levels of protection regardless of the ultimate destination of their data. The UK, in particular, will need to ensure that it transitions over existing third-country arrangements that it currently enjoys by virtue of it being a Member State of the EU. This will be necessary for both its own companies and consumers, but also so that organisations in the EEA will be able to better undertake onward transfers from the UK in compliance with GDPR.

For the EU, a close relationship with the UK should be pursued as the continued alignment of both jurisdictions in their approaches to data protection is in the interest of all UK and EU consumers and businesses. The relationship between the UK and the US will be of particular interest to the EU and it should be positive in its engagement with the UK to ensure that arrangements reached are satisfactory to all parties.

⁹⁵ See <https://www.ftc.gov/system/files/attachments/international-competition-consumer-protection-cooperation-agreements/140306ftc-uk-mou.pdf>

⁹⁶ See <https://www.justice.gov/opcl/judicial-redress-act-2015>

⁹⁷ See <https://www.justice.gov/opcl/privacy-act-1974>

⁹⁸ See http://europa.eu/rapid/press-release_IP-16-216_en.htm

⁹⁹ See <http://trade.gov/td/services/odsi/swiss-us-privacysield-framework.pdf>

Conclusion

The importance of maintaining the free flow of personal data between the UK and EEA post-Brexit cannot be overstated. With the European data economy expected to be worth €739 billion by 2020 the imperative to allow data to flow across borders is clear. Continued free flow of data between the EU and the UK will also ensure common, high levels of protection for citizens' personal data and, in the process, demonstrating that common standards can be pursued internationally.

Flows of personal data must be maintained through a secure and robust legal mechanism which provides certainty and clarity for the myriad of organisations and sectors whose customers rely on personal data crossing borders. This is not limited to the technology and financial industries.

As we have demonstrated, there are currently three options for facilitating data flows between the UK and EU post-Brexit. The EU and UK could: adopt mutual adequacy decisions; negotiate a bespoke relationship based on the UK Government's recent position paper; or businesses could rely on burdensome, expensive and unstable legal mechanisms or derogations.

The UK Government's position paper sets out a vision for a future data flows arrangement between the UK and the EU and industry welcome the aims and objectives of the paper. However, this approach is untested and therefore more detail is needed on how this would be achieved, including timing, legal certainty and how the potential political risks of this approach will be addressed.

If this option cannot be realised, the UK and EU should establish mutual adequacy decisions, alongside transitional arrangements, to ensure the free flow of data can continue as it does today. As mentioned throughout this report this would be of benefit to businesses and consumers across the UK and EEA. The remaining alternatives simply are not suitable, particularly for smaller businesses, given the costs and complexities of implementing them as well as some concerns around their legal fragility.

This report has set out the expected process the UK would have to pursue to secure an adequacy agreement and we believe, given the significant political, cultural, legal and economic links between the UK and EU, that the UK and EU begin from a strong starting point in finding each other adequate. The UK's implementation of the Data Protection Bill, and its commitment to the GDPR post-exit from the EU, is an important part of that process. However, the UK will also need to assess wider domestic legislation and regulatory considerations to ensure it is in the best possible position to achieve adequacy.

Given the above concerns, especially timing, the UK and EU should pursue mutual adequacy agreements, alongside transitional arrangements, to ensure the free flow of data can continue as it does today. As mentioned throughout this report, this approach would be of benefit to businesses and consumers across the UK and EEA. The remaining alternatives simply are not suitable, particularly for smaller businesses, given the costs and complexities of implementation as well as some concerns around their legal fragility.

This report has set out the expected process the UK would have to pursue to secure an adequacy agreement and we believe, given the significant political, cultural, legal and economic links between the UK and EU, that the UK and EU begin from a strong starting point for finding each other adequate. The UK's implementation of the Data Protection Bill, and its commitment to the GDPR post-exit from the EU, is an important part of that process. However, the UK will also need to assess wider domestic legislation and regulatory considerations to ensure it is in the best possible position to achieve adequacy.

Given that adequacy is not a quick process it is likely that transitional agreements will have to be implemented to avoid a “cliff-edge” scenario that would negatively impact businesses and consumers in both the UK and EEA. Transitional arrangements must ensure the continued free flow of data as today; be time-limited, ending once a future long-term data-sharing relationship has been implemented. In committing to GDPR following its exit from the EU the UK will oversee its own international data transfer regime. This should closely follow the European model and the UK must prioritise maintaining data flows to the EEA, through a mutual adequacy agreement, the US, through a UK-US Privacy Shield and other third countries already deemed adequate by the European Commission.

The flow of personal data is undoubtedly crucial to the future of growth in both the UK and EEA and must be maintained as it exists today. This report has set out a number of steps which, if followed, will secure that aim. Achieving the free flow of personal data between the UK and EEA is in the interest of consumers in both jurisdictions. We hope this can be secured to provide UK and EEA organisations of every size and sector with clarity and certainty that the free flow of data will not be disrupted so that they can continue to serve their customers on both sides of the channel.

Key recommendations: the need for a future data-sharing relationship to prevent disruption and enable growth.

The main recommendation of this report is that the EU and UK should pursue mutual adequacy agreements to provide a legal framework for the movement of personal data between the two jurisdictions.

This outcome requires the following actions:

- Both the EU and the UK should begin their adequacy assessment processes as soon possible.
- A standstill transitional arrangement for a set term in order to avoid a “cliff-edge” in the movement of personal data should be agreed immediately.
- The UK should consider implementing additional measures to ensure that any EU concerns about the UK’s data protection framework are addressed, particularly regarding processing of data for UK national security purposes.
- The UK should ensure that its ‘onward transfer’ regime, including with the US, provides equivalent levels of protection to those set out in the EU’s regime as this will form a key part of the EU’s adequacy assessment.

Annex – Alternative bases for international data transfers

In the absence of an adequacy agreement, or a new bespoke model for data flows, the established alternative legal bases, available at the business organisation level are:

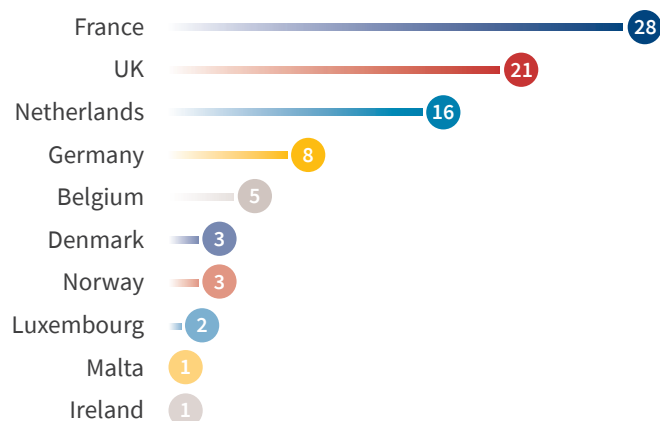
- Binding Corporate Rules,¹⁰⁰
- Standard Contractual Clauses,¹⁰¹
- Codes of Conduct,¹⁰²
- Certification,¹⁰³
- Derogations.¹⁰⁴

There are challenges, uncertainties, and disruptions associated with relying on such alternative arrangements for organisations in both in the UK and the EEA, especially SMEs. A detailed explanation of these alternative data transfer arrangements are below.

These alternative arrangements (other than the derogations from the GDPR requirements) are designed to ‘export’ or impose obligations that are substantially similar to European data protection law on the data recipients in the third country – the idea being that the alternative arrangements close any ‘gaps’ between the data protection and privacy laws of the third country and those of the EEA.

This Annex provides a detailed explanation of these alternative bases, as well as provide further information on adequacy decisions.¹⁰⁵ In doing so, it will highlight the challenges, uncertainties, and disruptions associated with these alternative arrangements. These are most prevalent for SMEs, both in the UK and the EEA. As will be made clear, implementing these alternatives is no easy task for organisations and they are not wide-ranging, and therefore adequacy is best suited to facilitate the frictionless free flow of data.

Approved BCRs



Binding corporate rules (BCRs)

BCRs are considered by privacy practitioners and many regulators as the data transfer ‘gold standard’, but they are generally only available for large multinational organisations.

BCRs allow large international organisations (or ‘undertakings’) to adhere to a common set of data protection policies that meet the standards laid out under European data protection law. These policies must be legally binding on all relevant entities within the international organisation’s group, and the BCRs themselves must be approved by the competent data protection authorities (e.g., the Information Commissioner’s Office in the UK). With BCRs in place, the entities in the group can transfer personal data between each other freely.

¹⁰⁰ See GDPR, Art. 47

¹⁰¹ See GDPR, Art. 46

¹⁰² See GDPR, Arts. 40 and 46

¹⁰³ See GDPR, Arts. 42 and 46

¹⁰⁴ See GDPR, Art. 49

¹⁰⁵ Different from the alternative data transfer arrangements, an adequacy decision does not impose any additional requirements on data recipients in a third country. As an exception, partial adequacy decisions impose additional obligations on participating companies – for example, the EU/US Privacy Shield Framework.

The steps for a successful BCR under the Data Protection Directive (DPD) include:¹⁰⁶

- **Map intragroup and external cross-border data flows** – This requires an organisational wide investigation of interconnected IT systems and data flows which can take several months.
- **Designation of a lead data protection authority (DPA)** – The organisation must identify its main establishment (the centre of its data processing activities) and complete part one of the BCR application.¹⁰⁷
- **Engage in initial negotiations with the potential lead DPA** – The lead DPA must agree to take on the BCR application. Once formally agreed, the lead DPA will identify two co-DPAs to assist with the BCR review as part of the mutual recognition process.¹⁰⁸
- **Prepare the BCR** – The organisation must (i) amend existing policies while drafting new policies based upon the findings in the audit; and (ii) establish a privacy governance framework to maintain the BCR. This process generally takes six months to a year.
- **Make the BCR binding** – The organisation must enter into an intra-group agreement, issue a binding board declaration, or otherwise take measures to give the BCR binding legal effect.
- **Submit the BCR** – The lead DPA works with the two co-DPAs to review the BCR. This typically takes a year of negotiations between the organisation and DPAs.¹⁰⁹
- **Activate the BCRs** – Once approved, the BCR is activated in each Member State by notifying the relevant DPA. Some data protection authorities may require an additional review. This process can take six months or more, depending on the individual DPAs.
- **Yearly review** – The organisation must go through an annual BCR review and notify the lead DPA of any material changes to the BCR over the course of the year (e.g., new members, changes in data privacy practices, etc).

Presently, only 88 companies have BCRs – 21 of those having been approved by the UK data protection authority.¹¹⁰ While a significant number of large organisations have successfully achieved BCR status (and a number more are progressing applications), this statistic reinforces the fact that BCRs are a limited solution for the vast majority of EEA and UK businesses.

Can BCRs ensure the free flow of data post-Brexit?

BCRs are a useful tool for large multinational firms. However, they have a number of limitations:

They are primarily used for transfers within a group which has multiple subsidiaries and affiliates globally to allow data transfers among those companies. BCRs can be used for transfers with external parties, but only in limited circumstances (e.g. Processor BCRs).

The process for obtaining BCRs, outlined above, is complex and frequently takes one to two years to complete. Anecdotally, some BCRs have taken upwards of five years to complete.

BCRs are costly to set up, putting them out of reach of SMEs.

In the experience of the authors of this report, BCRs (particularly when combined with preparatory data audits) require significant internal resources often incurring several hundred thousand Euros in external fees.

As such, BCRs, while useful to large multinational firms for internal transfers, have significant limitations and cannot provide a full solution to preserving data flows post-Brexit. They would not be appropriate for use by SMEs and therefore do not offer a universal solution that could be used by all organisations to ensure can continue to flow as it does today. Given the considerable lead-in time, BCRs will not be an effective tool to mitigate any “cliff-edge” risk associated with the UK leaving the EU in March 2019.

¹⁰⁶ See Article 29 Working Party Opinion Papers on Binding Corporate Rules, WP153, WP154, WP155, WP74, WP107, WP108, WP133, WP195 available at <https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/>. Please note, regulatory guidance is expected on the process for BCRs under the GDPR, particularly in relation to the GDPR's consistency mechanism.

¹⁰⁷ See Processor BCR Application (Art29 WP 195) available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195a_application_form_en.doc; Controller BCR Application (Art29 WP 133) available at https://ico.org.uk/media/for-organisations/binding-corporate-rules/1042458/wp133_bcr_application_form.pdf.

¹⁰⁸ See Art29 WP 107 available at https://ico.org.uk/media/for-organisations/binding-corporate-rules/1042454/binding_corporate_rules_cooperation_procedure.pdf

¹⁰⁹ See ICO guidance available at <https://ico.org.uk/for-organisations/guide-to-data-protection/binding-corporate-rules/>

¹¹⁰ See European Commission, List of Companies for which the EU BCR cooperation procedure is closed, available at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

Standard contractual clauses (SCCs)

SCCs are European Commission approved standard form agreements that impose contractual obligations on data recipients in third countries that are intended to mirror those obligations in European data protection law. They are the most common compliance tool used when transferring personal data to a recipient located outside of the EEA where no adequacy decision exists.

There are currently three different versions of SCCs:¹¹¹

- **controller to controller agreements** – of which there are two models; and
- **controller to processor agreements.**

New versions of SCCs that contemplate more complex data transfer scenarios are currently under development (e.g., processor to sub-processor clauses).¹¹²

Can SCCs ensure the free data flows post-Brexit?

While SCCs might seem like an option for cross border data transfers, they have several key weaknesses.

First, to use them effectively, companies must complete a complex network of SCCs. It is a challenging and time consuming process for a company to comprehensively and accurately ‘paper’ all cross-border data flows.

For example, suppose an organisation has three entities (including legal entities and branch offices) within Europe, five entities outside of Europe, and is using 80 vendor processors outside of Europe. At a minimum, this requires 15 intra-company SCCs amongst the entities within the organisation and 80 additional SCCs with the vendor processors – and that is only if the organisation takes the position that one SCC on behalf of all entities within the organisation is sufficient for the data transfers to each vendor processor. The internal and external costs of doing so can be upwards of several hundred thousand Euros.

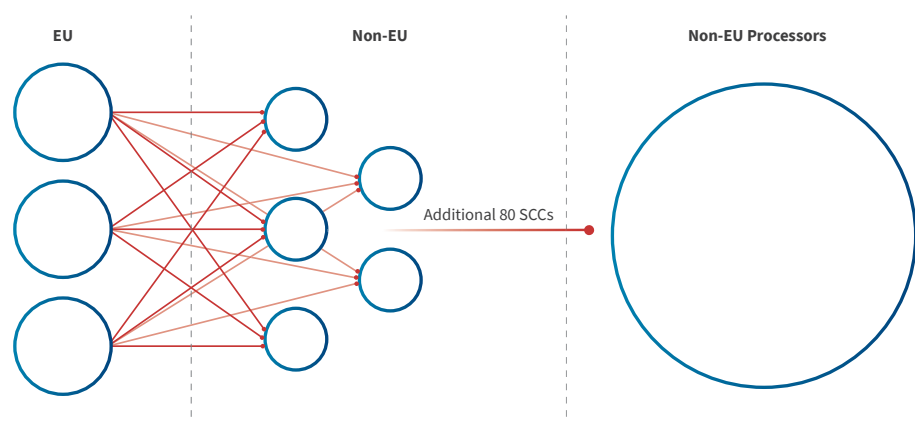
In practical terms, the process of entering into SCCs involves the following steps:

- **Map intragroup and external cross-border data flows** – This requires an organisational wide investigation of interconnected IT systems and data flows which can take several months.
- **Identify the appropriate SCCs to use in which specific circumstances** – This means reviewing the data mapping, identifying where data recipients are acting as controller or processor, and determining which SCC fits best.
- **Complete the SCCs** – The organisation will need to complete the SCCs by entering information about the contracting parties along with a description of the data flows which are to be covered by the SCC.
- **Sign the SCCs** – As there are frequently a large volume of SCCs, the process of gathering all of the signatures is somewhat time and labour-intensive. Certain territories may also require lodging of SCCs with the local regulator.
- **Review and further amendments** – The organisation will also need to continue to monitor its cross-border data flows, amending and entering into new SCCs where required, to match the changes in cross-border data flows.
- **Structural weaknesses** – It is not uncommon for data transfers to flow to cloud SaaS providers in the UK in the first instance, with onward transfer to sub-processor vendors outside of the EEA. Strictly speaking, the SCC does not anticipate this flow and stand-alone SCCs would need to be entered into with each non-EEA sub-processor vendor causing confusion and an internal management burden for a business.¹¹³

Similar to BCRs, a substantial amount of time, resources and financial cost is required by a business to implement a network of SCCs.

Second, when considering the role of SCC's as a viable alternative data transfer arrangement for businesses to use for cross border data flows after Brexit, it must also be highlighted that the robustness of current SCCs has been referred by the Irish courts to the CJEU.

From the graphic, we can see that managing the volume of SCCs can be complex, but so is the actual process of entering into SCCs.



¹¹¹ See http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

¹¹² See Article 29 Working Party Working Document http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp214_en.pdf

¹¹³ Guidance has been published to manage these challenges, but the solutions require internal assessment and resourcing, thereby increasing cost and potential delay https://www.privacycommission.be/sites/privacycommission/files/documents/01.01.01.41-wp176_0.pdf

Schrems 2 - Data Protection Commissioner v. Facebook Ireland Limited & Maximilian Schrems

On 31 May 2016, the Irish DPA commenced proceedings in the Irish High Court to seek a CJEU preliminary reference as to the validity of SCCs¹¹⁴ as the Irish DPA is not empowered to invalidate a European Commission decision on data transfers.¹¹⁵ That power is reserved for the CJEU and the European legislative process.

On 3 October a referral to the CJEU was obtained by the Irish High Court meaning that the CJEU will rule on the validity of SCCs, as it previously did with the EU/US Safe Harbor Framework under Schrems. If SCCs are held unlawful, all data transfers using existing SCCs will need to rely on another alternative data transfer basis or those data flows will be in breach of European data protection law.

Should SCCs be considered an invalid data transfer mechanism, either partially (e.g., when used for transfers to specific jurisdictions) or in full (e.g., as to any data transfers), then any cross-border data flows that are reliant on those SCCs will be immediately non-compliant with EU data protection requirements (unless an alternative lawful basis is available for those flows). This would result in a similar situation as was seen when the EU/US Safe Harbor Framework was invalidated in October 2015.

Third, there is further uncertainty caused by the GDPR itself. The existing three forms of SCCs today will very likely be replaced in time with updated SCCs that meet the standards of GDPR. It is not clear when this will occur, and any organisations entering into SCCs now face the very real possibility that they will need to replace their network of SCCs once again in the near future. Given that the UK is implementing the GDPR through the Data Protection Bill it is possible that a similar form of SCCs will be needed to allow data flows from the UK to third countries. There is a possibility that such clauses may diverge from EU SCCs, thereby potentially causing onward transfer compliance concerns.

Given the costs and complexity involved in implementing SCCs, which pose a particular challenge to SMEs, and the legal uncertainty associated with SCCs, they are a much more limited option than may initially appear. For smaller businesses with less access to costly legal advice there is a real risk that if SCCs are not fully understood, or overlooked, this could lead to non-compliance with the GDPR, resulting in significant financial penalties of up to 4% global annual turnover.

Codes of conduct

Codes of conduct are a form of self-regulation which serves as a valid data transfer mechanism under GDPR.

Codes of conduct allow industry associations to draft a code that will be binding on the members of that association (and therefore may be attractive in alleviating some of the regulatory burden of European DPAs).

Can codes of conduct ensure the free flow of data post-Brexit?

In theory, codes of conduct are a solution for data transfers within a particular industry. In reality, formally approved EU data protection codes of conduct are unprecedented.

Historically, there have been attempts at establishing codes of conduct, but these past attempts have taken several years, were filled with uncertainty, and ultimately, remain unresolved. For example, the Data Protection Code of Conduct for Cloud Service Providers went through four years of negotiations and has not yet resulted in a final valid Code of Conduct. It should also be noted that no previous codes have been aimed at providing a legal basis for the transfer of personal data from the EEA to a third country.

The envisioned process for a code of conduct under the GDPR is:

- **Industry Buy-in to Code of Conduct Process** – A trade association will need to gather and convince industry organisations to financially support the lengthy Code of Conduct process.
- **Draft and Submit the Code of Conduct to the Competent DPAs** – Once drafted by the trade association, the code of conduct must be submitted to the competent DPA but as the code of conduct will apply to an entire industry, it is difficult to predict how a competent DPA might be appointed.
- **Negotiate the Code of Conduct** – Once the DPA review process is established, there will be a need to engage with the DPA to negotiate the actual requirements of the code of conduct.
- **Consistency Mechanism** – The lead DPA must submit the Code for review by other data protection authorities and the EDPB.
- **Submission to the European Commission** – Once the DPAs and the EDPB have given a favourable opinion, the EDPB must then submit its opinion to the European Commission.
- **Commission Decision** – The European Commission will make a decision, through an implementing act, that will be adopted in accordance with the examination procedure.
- **Binding Commitments** – To benefit from the code of conduct, organisations will need to make binding and enforceable commitments to adhere to the code of conduct, likely through a contractual instrument.¹²¹

¹¹⁴ See <https://www.dataprotection.ie/docs/01-02-2017-Update-on-Litigation-involving-Facebook-and-Maximilian-Schrems/1598.htm>.

¹¹⁵ See Schrems, para 65 (<http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362>).

¹¹⁶ See European Commission, Data Protection Code of Conduct for Cloud Service Providers available at <https://ec.europa.eu/digital-single-market/en/news/data-protection-code-conduct-cloud-service-providers>

¹¹⁷ See GDPR, Art. 40(5)

¹¹⁸ See GDPR, Arts. 40(7) and 63

¹¹⁹ See GDPR, Art. 40(8)

¹²⁰ See GDPR, Art. 40(9)

¹²¹ See GDPR, Art. 40(3)

Codes of conduct may appeal to the EU negotiators as they are a much-promoted framework and (theoretically) can be deployed in respect of transfers globally within an industry. However they are just that – a solution limited to deploying industries that are unlikely to assist a wide cross-section of SMEs not falling within those industries and sectors. As such, they are not a solution for the UK and the EEA as a whole. This would not assist the multi-lateral data flows mentioned in this report where data flows between sectors and industries as well as across borders.

Given their limited scope to intra-industry transfers and the likelihood of long implementation timeframes codes of conduct are fraught with uncertainty, would involve a very lengthy drafting process without any guarantee of success, and are most likely not reasonably available for all industries. Consequently, it is highly unlikely that any code of conduct can act as an effective, universal solution for UK and EEA businesses following March 2019.

Certification

Similar to codes of conduct, certification is another form of self-regulation which serves as a valid data transfer mechanism under GDPR. Again, the key issue with certification for international data transfers is that it is unprecedented, and carries significant uncertainty.

Pursuant to GDPR, any Certification that is going to provide a data transfer solution would need to go through the following steps:

- **Formal accreditation of a certification body** – A certification body must seek formal accreditation by a competent DPA, the EDPB, and/or a national accreditation body in accordance with the Accreditation Regulation.¹²²
- **Accreditation process** – The certification body will need to (i) demonstrate their independence and expertise; (ii) agree to respect the certification requirements under the GDPR; (iii) establish a complaint handling procedure; and (iv) demonstrate that they are not under a conflict of interest.¹²³

- **Draft the mechanics of a certification scheme** – The certification body will need to draft the certification scheme, including the requirements of the certification scheme, how the certification scheme will be made binding on participants, and how redress mechanisms will function.
- **Approval of accreditation** – The certification body will need to enter into negotiations with the competent DPA and/or the EDPB to obtain formal approval of the certification scheme.¹²⁴
- **Approval of participants under the certification scheme** – Any controller or processor looking to participate in the certification scheme will need to apply. As part of this application, the controller or processor will need to provide any necessary documentation to the certification body to prove that the controller or processor complies with the certification scheme.¹²⁵ As this is a new and untested process, it is difficult to predict how long it might take.
- **Renewing certifications** – Certifications awarded are only valid for three years and must then be renewed.¹²⁶

Can codes of conduct ensure the free data flows post-Brexit?

In time, certifications may prove to be an attractive solution, particularly for SMEs, but at present, we are not aware of any accreditation bodies which might provide a GDPR data transfer certification nor are we aware of any substantive work commencing on what a certification scheme might involve.

Even if it was a current and available option, certification would still place the burden on the business to obtain compliance with the certification scheme. As with codes of conduct, it is very unlikely that a certification scheme for data flows between the UK and the EEA would be available by March 2019.

Derogations

In addition to the alternative data transfer arrangements discussed above, there are limited, fact-specific circumstances where personal data can be transferred to a third country without an adequacy decision and absent the transferring entities putting in place an alternative data transfer arrangement. These circumstances are set out as derogations to GDPR.

¹²² See GDPR, Arts. 43(1), 43(3); see also Regulation (EC) No 765/2008 available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0030:0047:en:PDF>.

¹²³ See GDPR, Art. 43(2)

¹²⁴ See GDPR, Art. 42(5)

¹²⁵ See GDPR, Art. 42(6)

¹²⁶ See GDPR, Art. 42(7)

Can derogations ensure the free flow of data post-Brexit?

The impact of the application of the derogations is that personal data is able to flow to a third country absent the protections afforded under the GDPR. As such, these derogations are largely only available for ad-hoc data transfers, on a case-by-case basis, and are not a viable solution for the habitual transfer of personal data. As the European Commission's advice states, derogations "cannot be presumed to apply to all conceivable situations" and within the GDPR, the derogations are specifically labelled as "derogations for specific situations".¹²⁷

Some commentators have suggested that data flows designed to combat financial crime or to provide medical benefits will be able to continue on the basis that the transfer is "necessary for important reasons of public interest".¹²⁸ One recital to the GDPR does provide for such transfers between public bodies (e.g., between financial authorities), but it does not account for transfers between private organisations (e.g., between branches of a financial institution). Further, recitals to the GDPR tell us that this derogation is limited to "important grounds of public interest laid down by Union or Member State law".¹²⁹ As such, post-Brexit, it would appear to be difficult for EEA entities to transfer personal data to the UK to combat financial crime or to provide medical benefits on the basis of public interest as these transfers are largely continuous, habitual, and based upon non-EU and non-Member State law.

The reality is that the derogations are only available for use in specific situations, most frequently in addition to other data transfer arrangements which are already in place. They cannot be relied upon by all organisations to enable the regular, free flow of data that exists today between the UK and EEA.

Adequacy

An adequacy decision concerning a third country by the European Commission means that the third country is considered to provide adequate protection for personal data (the GDPR recitals refer to "essentially equivalent"¹³⁰). Once a third country is determined "adequate" personal data may then flow from the EEA to the third country without the need to enter into any of the alternative data transfer arrangements discussed above.

This applies to all personal data transfers to recipients in the "adequate" third country, whether within the same business group or with external parties, and whether the firm is a large multinational or an SME.

Can adequacy ensure the free data flows post-Brexit?

Adequacy is by far and away the best option. It greatly reduces red tape around data transfers while still ensuring that personal data is protected and safeguarded. An adequacy decision avoids the need for additional costs and resourcing for organisations, is universal in application and would benefit all organisations equally.

¹²⁷ See GDPR, Art. 49

¹²⁸ See GDPR, Art. 49(5)

¹²⁹ See GDPR, recital 111. Indeed section 17 of the Data Protection Bill provides for the Secretary of State to issue regulations explaining when these circumstances would apply.

¹³⁰ See GDPR, recital 104

Frequently Used Terms

Bilateral Agreement	Any new partnership agreement (including any free trade agreement) concluded between the EU27 and the UK, under which there is a higher level of reciprocal liberalisation of trade between them than they provide to most other countries through their WTO commitments.
Charter of Fundamental Rights	One of the general principles of EU law is respect for fundamental rights, which includes many of the rights we refer to as human rights in the UK. The EU codifies fundamental rights in the Charter of Fundamental Rights of the European Union, which has the same legal status as the EU treaties. The UK Government has signalled that the Charter will not be converted into UK law by the European Union (Withdrawal) Bill.
Data Protection Bill	The UK Data Protection Bill [HL], introduced into the House of Lords on 13 September 2017.
Data Protection Law Enforcement Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.
ECHR	European Convention on Human Rights. The ECHR is an instrument of the Council of Europe, not of the EU. In the European Union (Withdrawal) Bill white paper the UK Government stated that UK's withdrawal from the EU will not change, for now, the UK's participation in the ECHR and that there are no plans to withdraw from the ECHR.
Essential equivalence	Essential equivalence is the current test used to determine whether a third country is an adequate destination for personal data, and (pursuant to the Schrems case) it requires that all laws of the third country shall be considered when determining adequacy – not merely data privacy laws. Once GDPR is in force, the current essential equivalence test will be bolstered by the Art. 45(2) adequacy assessment criteria.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation). This Regulation will come into force within the EEA (including the United Kingdom) on 25 May 2018.
European Union (Withdrawal) Bill	The UK Government has proposed that the constitutional and legal consequences of the UK leaving the EU will be implemented by the European Union (Withdrawal) Bill. ¹³¹ This will annul the European Communities Act 1972, which incorporates EU law into UK law. At the same time, it will transpose EU law as at the date of exit into UK law so that there is legal continuity. There may be provisions enabling Ministers to subsequently repeal individual EU law provisions by secondary legislation, or alternatively this may be affected by subsequent primary legislation.
Schrems	Case C-362/14, Judgment of the Court (Grand Chamber) of 6 October 2015, Maximilian Schrems v Data Protection Commissioner.
Withdrawal Agreement	The withdrawal agreement between UK and EU, as contemplated under Article 50 of the Treaty on European Union.

131 See Department for Exiting the European Union, *Legislating for the United Kingdom's withdrawal from the European Union* available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/604516/Great_repeal_bill_white_paper_accessible.pdf

Glossary

A29WP	Article 29 Working Party
BCRs	Binding Corporate Rules
Court of Justice of the European Union (CJEU)	The Court of Justice of the European Union interprets EU law to make sure it is applied in the same way in all EU countries, and settles legal disputes between national governments and EU institutions
Data Protection Directive (DPD)	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
DE Act	Digital Economy Act 2017
DPA	Data protection authority (a supervisory authority under GDPR)
EEA	European Economic Area
EFTA	European Free Trade Association
EFTA Court	The EFTA Court fulfils the judicial function within the EFTA system, interpreting the Agreement on the European Economic Area with regard to the EFTA States party to the Agreement. At present those EFTA States are Iceland, Liechtenstein and Norway
EU	European Union
IP Act	Investigatory Powers Act 2016
SCCs	Standard Contractual Clauses
TFEU	Treaty on the Functioning of the European Union

Disclaimer and Copyright

This report is intended to provide general information only and is not intended to be relied on as a comprehensive guide or to provide legal or other advice. You should not take, or refrain from taking, action based on its content. Information contained in this report was obtained from third party law firms and/or public sources. No presentation or undertaking is made or given by any person as to the accuracy, completeness or reliability of this report or the information or views contained in this report. None of the UK Finance, techUK, Dentons, or any of their respective partners, principals, employees, members, agents or contractors shall have any liability or obligation to any person arising from or in connection with any use, or misuse, or reproduction of this report or any information or views contained in this report. Neither Dentons, UK Finance or techUK undertakes any responsibility to revise or update this report or otherwise to communicate to any person any inaccuracy in this report that is identified, whether as a result of new information, future events or otherwise.

© 2017, NewTA Limited trading as UK Finance, techUK, Dentons UKMEA LLP
