Brexit Quick Brief #5

Data protection and transfer

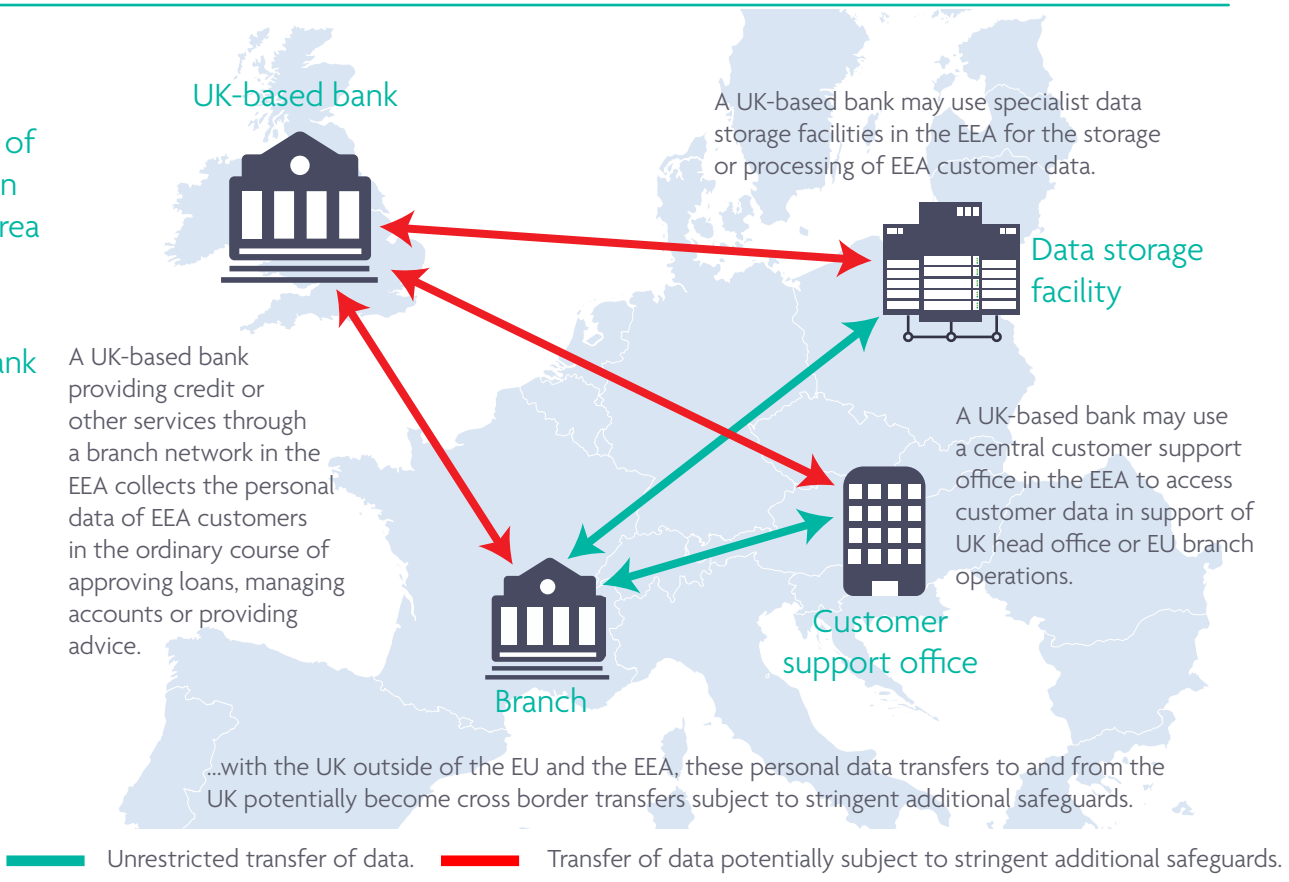
UK FINANCE

Key points

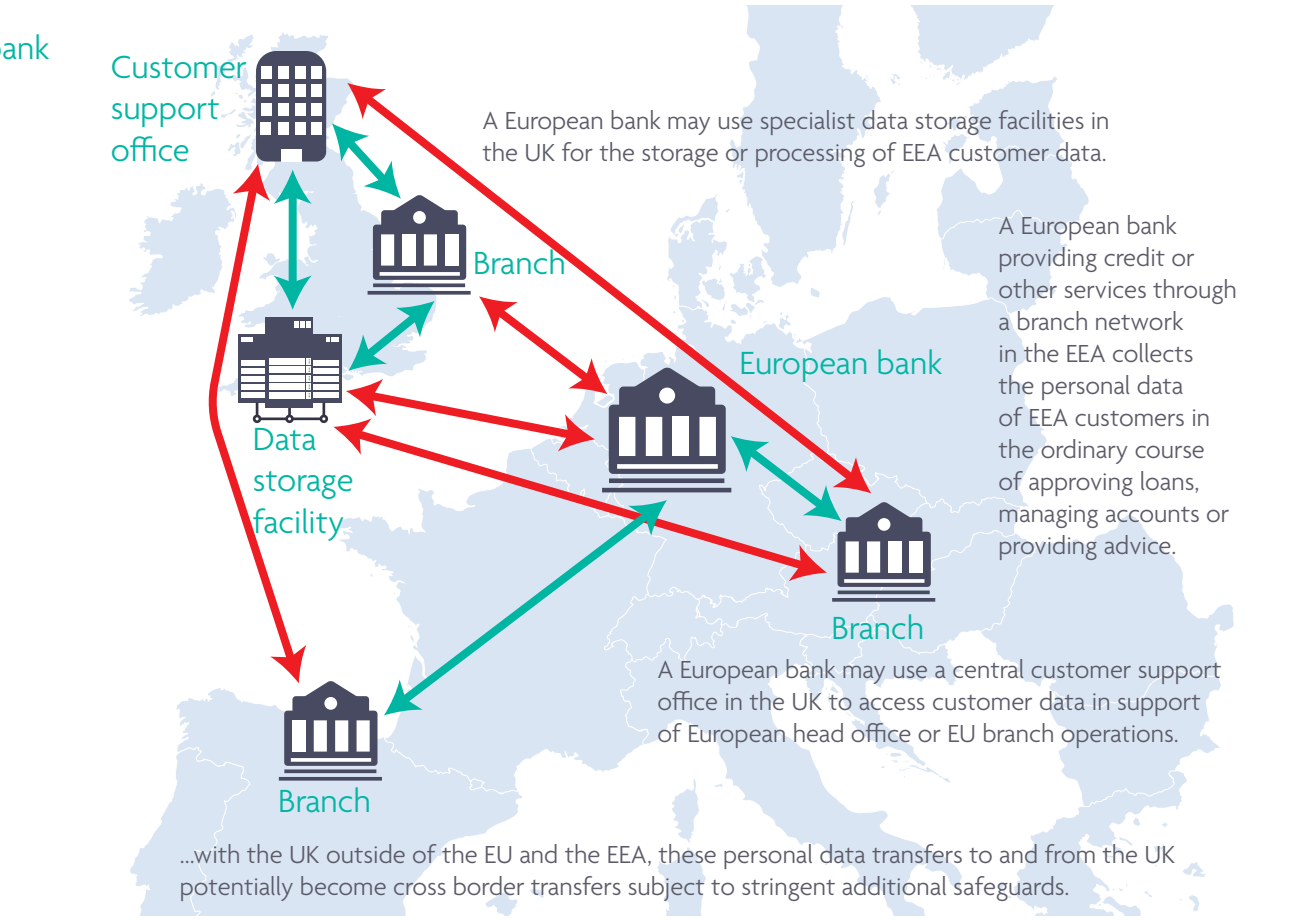
- The movement of personal data between locations is an integral part of modern banking operations. Financial services firms store and process personal data digitally as part of conducting business, including operating retail and corporate accounts, providing lending, securities operations, investments, preventing financial crime and as part of workforce management.
- In the modern digital economy, moving personal data between the UK and EEA is an important part of a huge range of sectors far beyond financial services and banking. Any and all businesses that move personal data between the EEA and the UK will potentially be impacted by a disruption in the legal framework that permits this movement.
- Within the EEA the processing of personal data is governed by the EU data protection regime, which protects individuals' privacy and other information rights. This regime permits the intra-EEA transfer of personal data. Many banks and other companies in the EEA have taken advantage of this framework to rationalise processing, or to provide customer service or back office functions, from a limited number of locations inside the EEA.
- Recent regulation and legal precedent have expanded 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 the movement of data, and the value that is derived from those flows.
- Following the UK's exit from the EU, a new relationship for the movement of personal data will be required between two legal frameworks based on the mutual goal of ensuring a high standard of protection for citizens' personal data.
- The EU applies significant safeguards on personal data transferred out of the EEA. The EU will replace such restrictions with a general permission to move data where it has recognised the data protection standards of another country as 'adequate'.
- Adequacy is a legal determination defined in EU data protection law. Its benefit to firms is that the process of an adequacy decision creates a robust legal status.
- For the UK and the EU to each agree the adequacy of their respective data protection regimes after the UK exit from the EU may not be straightforward. The UK and EU should thus begin their adequacy assessment processes as soon as possible.
- Timing is a concern for a mutual adequacy agreement between the UK and EU. This raises the clear risk of a "cliff-edge" for thousands of exposed companies and their customers. The EU and UK should agree to a standstill transitional arrangement for a set period to allow time for mutual adequacy agreements to be put in place.
- Firms in the UK and EEA will need early notice of an adequacy agreement or transition arrangements or they will need to develop new systems for ensuring compliance with restrictions on personal data transfer between the UK and the EU.
- A framework will also be necessary to ensure that data transfers between the UK and non-EEA countries can continue securely and efficiently. The UK will need to replace the existing data transfer frameworks created by the EU's previous recognition of other countries' data protection regimes. The robustness of these UK regimes, especially with the United States, may be a factor in the willingness of the EU to recognise the UK's own framework as adequate. Therefore, the UK should ensure that its international and 'onward transfer' regime, including with the US, provides equivalent levels of protection to those set out in the EU's regime.
- The UK Government has proposed a bespoke approach to the future data protection relationship based on the existing adequacy model. While the aims and objectives of the UK's approach are satisfactory, more detail is needed on how those aims will be achieved particularly in the areas of timing, legal certainty and political risk.

UK Finance Quick Briefs are a series of short papers intended to inform readers about key commercial, regulatory and political considerations around Brexit. While they are focused on banking, many of the issues discussed have wider relevance. Each BQB may be read on its own or in conjunction with other papers in the series. It is intended to expand the series as further topics of significance are identified.
For further information on Quick Briefs visit:
www.ukfinance.org.uk/quickbriefs

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



EU-based bank



Movement of data in the European Economic Area

The movement of personal data between locations is an integral part of all modern financial services. Banks and other financial services businesses store and process personal data digitally as a routine part of conducting business, including providing lending, securities operations, investments, client due diligence, operating retail and corporate accounts and complying with regulatory requirements like preventing money laundering and terrorist financing. They move this data between locations, often for processing in specialist facilities. This can be individual customer data, employee data or business customers' data where this relates to, for example, the business customer's directors or employees.

In an increasingly digital economy, movement of data within and across businesses is an everyday part of a huge range of sectors far beyond banking and financial services. Further, recent regulation and legal precedent has expanded 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 the movement of data, and the value that is derived by many businesses in different from those flows.

How is personal data transferred across the European Economic Area?

Many banks and other companies in the EU have rationalised data storage or processing, or the provision of customer service or back office functions, into centralised locations inside the EU.

Within the EEA the transfer of personal data across national borders is governed by the EU data protection regime, which permits intra-EEA transfers. At the centre of this, the EU's Data Protection Directive (DPD) sets minimum standards for accessing, storing, processing and transferring the personal data of EU/EEA individuals so as to protect their rights and interests, particularly their privacy. Provided businesses observe these data protection requirements, they are free to move the personal data of customers or employees throughout the EEA Member States. Not only does this underpin a wide range of everyday activities, but many banks and other companies in the EEA have taken advantage of this framework to work more efficiently and effectively by rationalising data storage or processing, or to provide customer service or back office functions, from centralised locations inside the EEA.

The EU data protection framework is currently in the process of being revised. The DPD will be replaced in mid-2018 when the new EU General Data Protection Regulation (GDPR) enters into force. The GDPR introduces more stringent requirements for businesses in many areas and centralises a number of aspects of EU data protection at the EU level, including responsibility for assessing the adequacy of data protection frameworks of non-EU countries. The GDPR also introduces a more centralised system of regulation and an arbitration system between national data protection authorities where they disagree. However, it continues to provide for a high level of freedom in moving personal data freely between companies or other organisations in the EEA – subject to rigorous protection rules for personal data and especially stringent protections for 'sensitive personal data' related to matters such as an individual's health, criminal record or race.

How is personal data moved out of the European Economic Area?

Leaving the EU and the EEA would move the UK outside of the EU data protection framework. Both the DPD and the GDPR allow for data of EU/EEA individuals to be transferred outside of the EEA provided that they are afforded an adequate level of protection. The EU allows this in two ways:

- Through a series of additional safeguards applied by companies moving personal data to countries outside the EEA. These can involve a range of potentially complex obligations additional to standard data protection practice, including requirements to seek customer consent for any cross-border transfer of their data outside the EEA, or the use of standard contractual clauses to authorise cross border data transfers or
- Through an assessment of the data protection rules in the jurisdiction to which data is being moved that judges them 'adequate' to EU standards in terms of law, practice and supervision. This is essentially a variation of the 'equivalence' judgements (see BQB #4: What is equivalence and how does it work?) that are a common feature of EU rules in other areas. This assessment is currently conducted by the European Commission and informed by the EU's national data protection authorities, a model that is broadly maintained by the new regulations. The process for determining adequacy is defined in EU data protection regulation and an adequacy decision has the effect of creating a robust legal status.

Implications – alternatives and the 'cliff edge'

Transitional arrangement are needed to avoid a damaging 'cliff edge' effect in the movement of data between the EU and UK.

Following the UK's exit form the EU, a new relationship for the movement of personal data will be required between the two legal frameworks based on the mutual goal of ensuring a high standard of protection for citizens' personal data. Agreeing this new relationship will not be easy in the time allowed by the Brexit negotiations. In theory, the existing right to move such data freely between the UK and EEA could lapse overnight at the point of the UK's exit, creating serious risk of disruption to businesses, customers and employees whose services currently depend on this freedom.

Given the timing concerns, avoiding uncertainty on this point will only be possible via transitional arrangements that preserve the acquis for a set period. Such arrangements will allow the UK and EU time to agree their future data-sharing relationship which we believe should be in the form of mutual adequacy agreements.

Without certainty of this kind well in advance of the UK's exit, UK and EEA firms will need to ensure compliance by using one of the alternative safeguards for transfers. However, these all have drawbacks. As a result, and in order to ensure they can continue necessary processing, firms may need to move data processing activities between countries, consider the relocation of their data centers and / or implement other procedures to avoid problematic cross border transfers of personal data.

An EU 'adequacy' decision

There is no legal reason why the adequacy assessments cannot begin while the UK remains an EU member

An 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 within the EU. This concept of "essential equivalence" does not require identical law, but laws which offer the substantially same level of protection. To ensure success the UK may want to consider customised data protection commitments similar to what was agreed in the US-EU Privacy Shield (see box 1: the US, the UK and data protection adequacy from the EU perspective).

The UK will also need to assess the EU's regime as 'adequate' to satisfy the requirements of the UK Data Protection Bill. For the UK and the EU to each agree the adequacy of their respective data protection regimes after the UK's exit from the EU may not be straightforward. Foreseeing this potential, the UK and EU should begin their adequacy assessment processes as soon as possible. It is our understanding that there is no legal reason why the adequacy assessments cannot begin while the UK remains an EU member.

Box 1: The US, the UK and data protection adequacy from the EU perspective

It might be assumed that as a former EU Member State it would be straightforward to the UK to be judged by the EU to be 'adequate' for the purposes of data protection rules. This may not be the case. The UK Government opposed some of the requirements in the GDPR and will likely make use of many of the areas of national discretion permitted by the Regulation. For example, in February 2016 the UK Government announced it would opt out of a GDPR provision restricting the disclosure of personal data to foreign courts or regulators. While such flexibility may be permitted inside the EU as a tradeoff granted to the UK as a Member State with established reservations in this area, as a third country outside the EU, such differences will inform its prospects of being deemed 'adequate' by the EU.

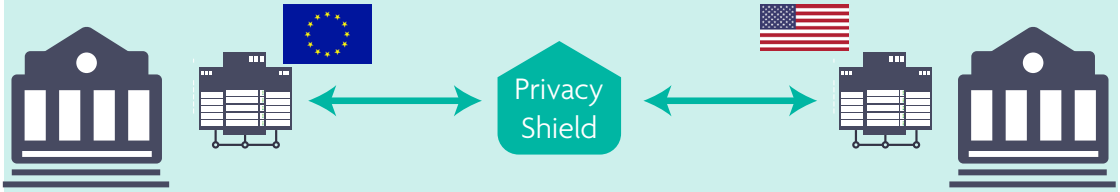
The recent history of EU – US data transfer rules clearly demonstraight the potential risk and disruption for business.

- The EU and US attempted to bridge divergences in data protection practice with a customised agreement based on US commitments to protect EEA citizen data: the 'Safe Harbour' framework. This was necessary due to the absence of general data protection legislation in the US. The framework enabled US businesses that were regulated by the Federal Trade

Commission (FTC) to sign up to it and agree to be bound by the framework's data protection principles. This EU-US agreement was overturned in the courts and led to firms in the EEA, who had relied on the framework to lawfully share information with US organisations, being suddenly in inadvertent breach of data protection requirements, and having to urgently review and update contracts with US firms; a task of significant complexity. Certain firms failed to adapt and have been fined by EU-based data protection authorities.

2000 - EU-US Safe Harbour agreement provides a legal framework for US companies to move EU/EEA personal data to the US subject to self-regulated principles of data protection.

2015 - The Safe Harbour agreement is struck down by the Court of Justice of the European Union (CJEU) for inadequate guarantees of data protection. The EU assessments of the US for adequacy under the Data Protection Directive continue to identify significant variation in the protection afforded by the two regimes.



2016 - The EU and the US negotiate the 'Privacy Shield' agreement containing customised data protection commitments from the US for EU/EEA personal data to allow an adequacy finding for the US regime. This agreement may still be challenged in EU courts.

- The very similar replacement agreement – the EU-US 'Privacy Shield' – is intended to address the Safe Harbor shortcomings. However, it has also been legally challenged on the grounds that this has not been achieved, and data protection authorities have flagged similar concerns. The chances of Privacy Shield being successfully overturned remain uncertain, but could increase depending on the actions of the new US administration. Many US firms in the EU have indeed chosen not to rely on the Privacy Shield due to uncertainty as to its future. Whilst businesses, including the financial sector, not regulated by the FCC can put in place arrangements and safeguards to allow data to be shared, these may make it more difficult, more expensive and carry a greater legal risk.

Safe Harbor and Privacy Shield demonstrate some of the difficulties about reaching a decision of adequacy and highlight issues that may arise in discussions between the UK and EU about adequacy. If there is a perception among other EU states that broader elements of the UK's legal and law enforcement framework are not compatible with relevant EU principles, this could lead to challenges to any adequacy decision in the CJEU or in political pressure against maintaining the UK's adequacy standing.

Establishing a new UK framework for cross border data transfers

The UK will also need to replace the existing data transfer arrangements created by the EU's previous recognition of data protection regimes in other countries.

Transfer of personal data between the UK and other third countries.

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'.

A new framework will thus be necessary to ensure that data transfers between the UK and non-EEA countries can continue securely and efficiently. To achieve this the UK will need to replace the existing data transfer arrangements created by the EU's previous recognition of other countries' data protection regimes in countries including Argentina, Canada, Israel, New Zealand and Switzerland.

The UK has said that it will "liaise with those third countries to ensure that existing arrangements will be transitioned over at the point of exit". The robustness of these replace with arrangements, especially with the United States, may be a factor in the willingness of the EU to recognise the UK's own framework as 'adequate'. Therefore, the UK should ensure that its international and 'onward transfer' regime provides equivelent levels of protection to those set out in the EU's regime. Regarding the US, the UK may need to enter into its own 'Privacy Shield' arrangement in order to ensure proper protections for UK personal data and facilitate transfers.

Transfer of personal data from other countries to the UK.

The UK's own regime will also need to be assessed by a number of countries that impose their own restrictions on cross border transfer of personal data including markets such as Japan and Israel. Some countries look to the EU's list of adequacy agreements to inform their own list of countries that have 'adequate' protection, so that the EU's findings in relation to the UK would influence the findings of other countries outside the EU.

Summary

It is the view of the financial services industry that the EU and UK should pursue mutual adequacy decisions to provide a legal framework for the movement of personal data between the two economies. 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 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; and
- the UK should ensure that its international and '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.

See also

BQB # 1 Staying in or leaving the EU Single Market.
BQB # 2 An orderly exit from the EU.
BQB # 3 What is 'passporting' and why does it matter?
BQB # 4 What is equivalence and how does it work?
BQB # 6 Time to adapt – the need for transitional arrangements.
BQB # 7 The Repeal Bill - providing certainty and continuity
BQB # 8 External trade policy and a UK exit from the EU - clarifying the UK's WTO profile and beyond.
BQB # 9 Impact of Brexit on cross-border financial services contracts