Brexit Quick Brief #5

The voice of banking

Data protection and transfer

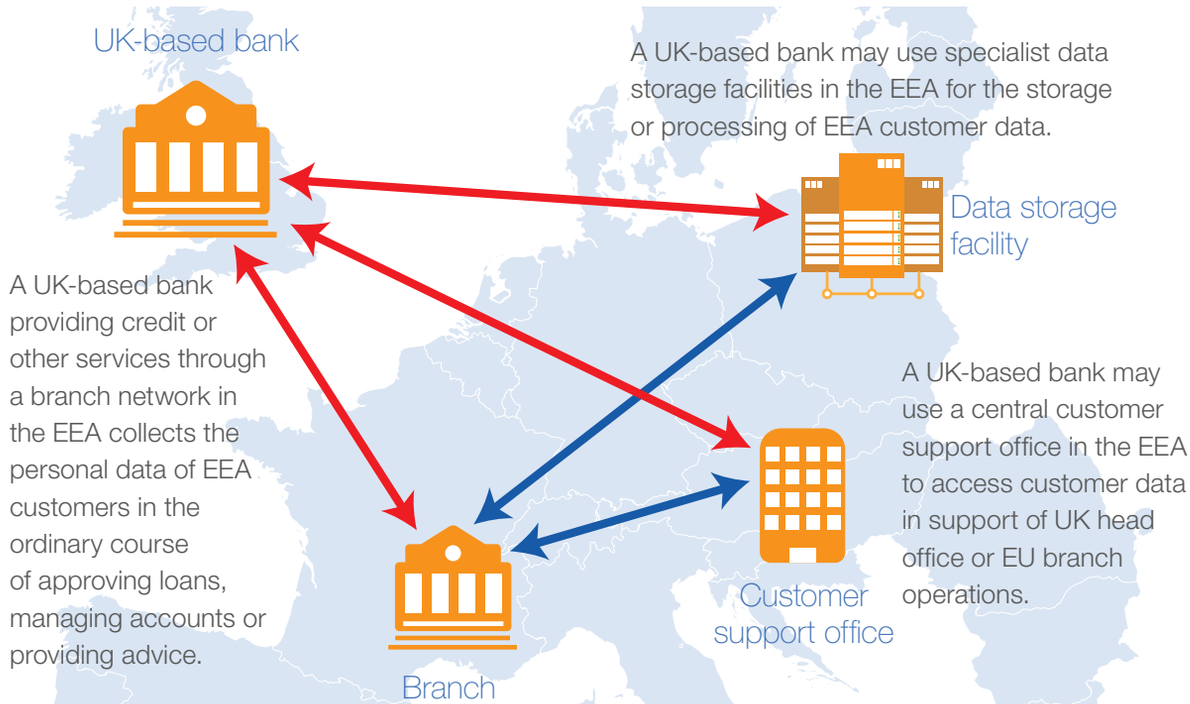
BBA Brexit Quick Briefs are a series of short papers intended to inform readers about key commercial, regulatory and political considerations around Brexit. While they are focused on banking, many of the issues discussed have wider relevance. Each BQB may be read on its own or in conjunction with other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

Key points

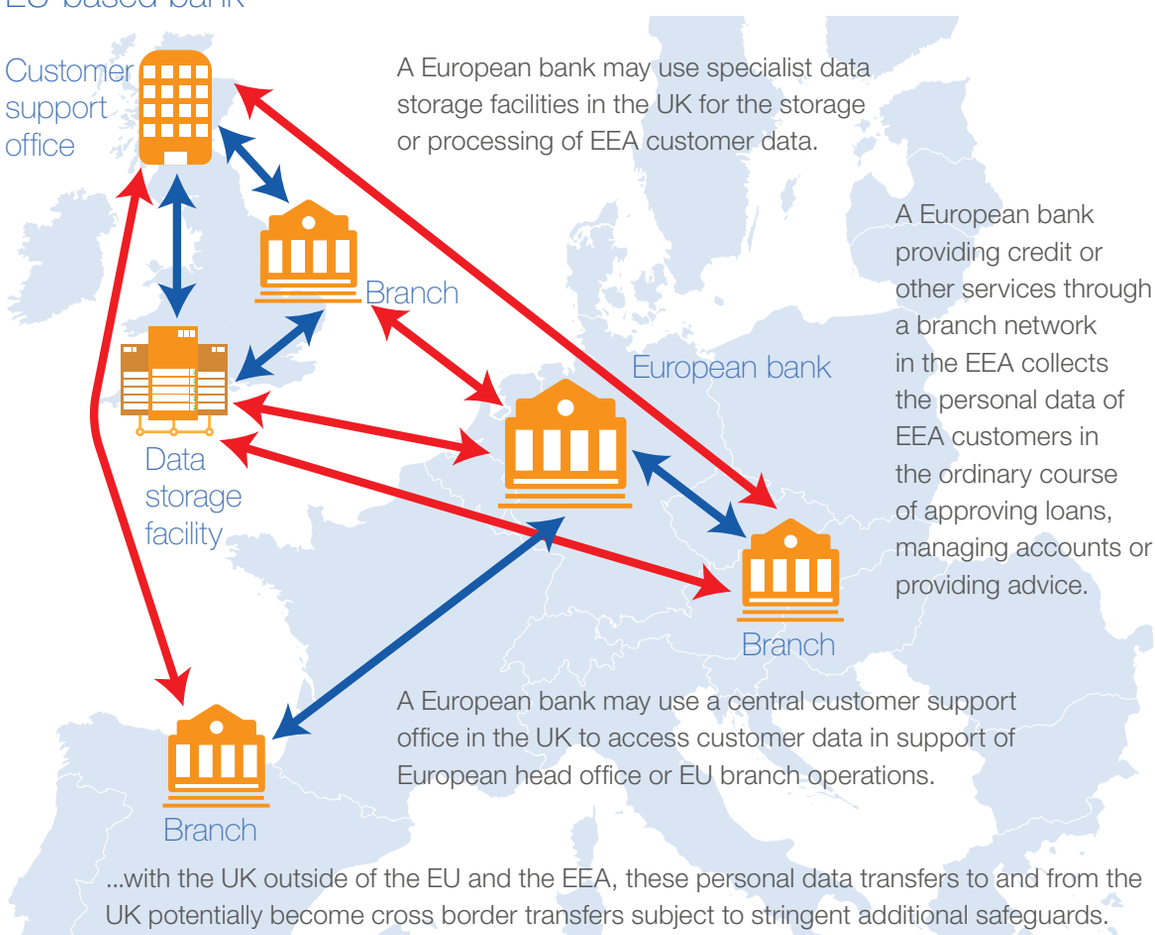
- The movement of personal data between locations is an integral part of modern banking operations. Financial services firms store and process personal data digitally as part of conducting business, including operating retail and corporate accounts, providing lending, securities operations, investments, preventing financial crime and as part of workforce management.
- Within the EU and 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 EU 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 EU/EEA.
- Following the UK exit from the EU, both the UK and the EU have a shared interest in ensuring the efficient transfer of data in an increasingly digitised world where the movement of data is part of everyday business.
- The EU applies significant safeguards on personal data transferred out of the EU which can be complex and resource intensive to administer as well as being at risk of legal challenge. 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'.
- 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 US experience of agreeing data protection adequacy frameworks with the EU suggests some of the potentially difficult issues ahead.
- Even if an adequacy decision can be reached, this may take some time to achieve. Transition arrangements may therefore be needed.
- Without an adequacy agreement, or even ahead of one if there is not a transition arrangement put in place to bridge the gap, firms will need to develop new systems for ensuring compliance with restrictions on personal data transfer between the UK and the EU. It will be important for businesses in all sectors to review how they, and third parties in their supply chain, will ensure they are compliant as there is no one model for achieving compliance. It could be a complex task and could involve relocating some operations.
- These issues have material implications far beyond banking and financial services – any and all businesses that move personal data between the EU and the UK are potentially impacted.
- A framework will also be necessary to ensure that data transfers between the UK and non-EU countries can continue securely and efficiently.

Transfer of data across and outside of the Single Market

UK-based bank



EU-based bank



Unrestricted transfer of data.

Transfer of data potentially subject to stringent additional safeguards.

Movement of data in the EU Single Market

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.

The movement of personal data between locations is an integral part of all modern banking 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.

How is personal data transferred across the EU single market?

Within the EU and 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 EU and EEA Member States. Not only does this underpin a wide range of everyday activities, but many banks and other companies in the EU 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 EU.

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 EU and 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 EU?

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 special model contracts to authorise cross border data transfers (see Table 1: Data transfer options compared); 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. A number of non-EU countries including Switzerland, Argentina, Israel and Canada have such adequacy determinations. The EU itself has also been granted adequacy determinations by a range of countries that otherwise restrict cross border data transfers.

Implications – alternatives and the 'cliff edge'

Exit from the EU will require appropriate protections in the UK for the data of EU/EEA individuals and vice versa as well as an efficient means to transfer personal data between the jurisdictions. Both the UK and the EU have a shared interest in ensuring the continued efficient transfer of data in an increasingly digitised world where the movement of data is part of everyday business.

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

In theory, the right to move such data freely between the two jurisdictions could lapse overnight at the point of UK exit from the EU, creating serious risk of disruption to businesses, customers and employees whose services currently depend on this freedom. Avoiding uncertainty on this point will only be possible via transitional arrangements, or an adequacy determination from the UK and the EU in respect of each others' data protection regimes.

Without certainty of this kind well in advance of UK exit, UK and EU 27 firms will need to ensure compliance by using one of the alternative safeguards for transfers. However, these all have drawbacks (see Table 1: Data transfer options compared). 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

Securing such an adequacy determination from the EU will require that the UK maintain a data protection framework sufficiently aligned with that of the EU to be judged comparable. This involves an assessment of more than just the data protection laws themselves, and may not be straightforward (see Box 1: the US, the UK and data protection adequacy from the EU perspective).

Securing an adequacy determination with the EU on data protection may not be straightforward.

The GDPR is only one area where the UK will need to consider careful alignment with the EU on data protection. Another is its transposition of the cybersecurity frameworks in the Network and Information Security Directive (NISD). These create duties for companies, including banks and market infrastructure firms, for protecting themselves against cyberattacks and protocols for sharing data about cyberattacks between EU authorities. The UK may need to develop systems for similar cooperation outside of the EU. Moreover, continued alignment with NISD standards may be part of a future EU adequacy judgement on the UK for data protection.

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

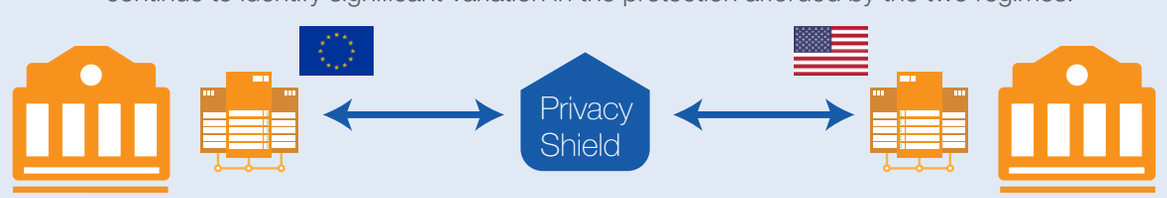
It might be assumed that as a former EU Member State it would be straightforward to the UK to be judged by the EU to be "adequate" for the purposes of data protection rules. This may not be the case. The UK Government opposed some of the requirements in the GDPR and will likely make use of many of the 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 data protection principles. This EU-US agreement was overturned in the courts and led to firms in the EU, 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 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 if one is required 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 Court of Justice of the European Union (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 need to establish a new framework for cross border data transfer that is currently covered by EU rules.

- Transfer of personal data from the UK to the EU/EEA

The UK will need to develop its own framework for recognising the data protection standards of the EU as adequate for the transfer of personal data from the UK to the EU/EEA. This will be important both for banks and other companies in the UK wishing to move the personal data of UK individuals to service centres or other sites in the EU/EEA for processing or storage.

- Transfer of personal data from the UK to other countries

The UK will also need to replace the existing data transfer frameworks created by the EU's previous recognition of data protection regimes in countries including Argentina, Canada, Israel, New Zealand and Switzerland. It will also need to consider its data protection framework with the US. The UK may need to become a party to the 'Privacy Shield' or set up its own bilateral arrangement in order to ensure proper protections for UK personal data and facilitate transfers. In the absence of such a bilateral arrangement, UK firms will need to employ alternative safeguards to make transfers. These are likely to be complex, potentially less robust and may be time consuming to administer. 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.

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

- 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 'adequate' countries to inform their own list of countries that have adequacy protection, so that the EU's findings in relation to the UK would influence the findings of other countries outside the EU.

Table 1: Data transfer options compared	
The scope to move personal data…	
...Within the EEA and EU or from the EEA and EU to countries outside with a data protection adequacy decision in place.	Personal data can be moved freely between countries, subject to meeting data protection requirements in both jurisdictions.
…From the EEA and EU to countries outside without a data protection adequacy decision.	Where no EU data protection adequacy decision is in place for a country outside the EEA, companies may still move personal data to entities in those countries, provided they have implemented one of a range of additional safeguards. These can include: • Model contracts. If they are legally able to contract with each other, the data sender and recipient can agree a model contract on data protection terms for transfer between them. This contracting model raises some issues for banks and their branches, which are part of a single entity. Also, some banks are likely to have hundreds or even thousands of contracts to review if they take this approach. In addition, a legal challenge against the legitimacy of model contracts is currently before the courts. • Binding Corporate Rules (BCRs). Where a company can demonstrate to EU data protection authorities that high levels of data protection are observed consistently and robustly across all of its global operations, these may be recognised as providing sufficient guarantee of personal data protection to allow cross border transfer of data between parts of such a company. These can be complex and time-consuming to design and secure, and need to be continuously updated. • Additional client disclosures and requests for authorisation. Companies may seek customer 'explicit consent' for transfers of their data out of the EU. However, this poses challenges for many types of transfer. For example, where a transfer is required for regulatory purposes, a bank could not run the risk that the customer might refuse to consent or might later withdraw consent to recurring transfers, putting the bank in breach of its obligations.

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?