



AMI Factsheet: Brexit

Introduction

This AMI factsheet is designed to provide member firms with information on areas that should be considered and reviewed ahead of the end of the UK's EU withdrawal transition period (this ends at 11pm on 31 December 2020).

These are some of the areas that may impact member firms:

- The loss of passporting rights.
- Data protection.
- Employing EU citizens in the UK.

Loss of passporting rights

The current passporting system (the ability of firms in one member state to carry out activity in another member state without requiring local authorisation) will no longer apply after 31 December 2020.

An alternative to passporting rights (although not comparable) is equivalence. HM Treasury has granted the EU equivalence in a number of areas that affect financial services and this will allow UK customers to continue to receive services from EEA* firms. However, at the time of writing the EU has not yet made any equivalence determinations on the UK (apart from one on central counterparties as that is a matter for financial stability).

This means that if you are a UK firm with customers who are based in the EEA, after the transition period comes to an end the extent to which you can provide services to these customers is a matter of local law and regulation in each jurisdiction.

Broadly speaking general servicing (e.g. normal administrative activities and general communications) of EEA based customers who have a mortgage on a UK property is likely to be permissible. However, the risk is that EEA countries may have differing rules and regulations on areas such as cross-border communications and what constitutes the servicing of a customer, which mortgage intermediary firms could fall foul of. Therefore, it is important that firms with customers in the EEA review and

*European Economic Area. EEA includes EU countries and also Iceland, Liechtenstein and Norway.

The contents of this guidance do not constitute legal or other professional advice. Users should seek appropriate legal guidance before coming to any decision or either taking or refraining from taking any legal action. AMI disclaims all liability for loss and/or damage that may result from its use.

understand the local laws and regulations in each of the relevant jurisdictions, speak to local regulators and consider legal advice.

Recommendations have been made that if a customer took out a product/service in the UK and has moved cross border it is treated as a UK contract. However, these are recommendations only and firms cannot assume that this will be the case.

If a firm currently relies on a passport to provide services to or from the UK, and proposes to cease those services at the end of the transition period, the FCA expect firms to ensure the right outcomes for customers, and provide timely communications to enable them to make appropriate decisions. More details on the FCA's expectations on communications with customers can be found [on this page](#).

FCA has published pages on [preparing your firm for Brexit at the end of the transition period](#) and [considerations for UK firms](#). These should be viewed alongside the other FCA Brexit communications, which can be found [here](#).

We are aware that to date many lenders have not communicated their stance on those customers who have a mortgage in the UK but live in the EEA. We have asked IMLA to raise this with their members and provide clarity to mortgage intermediary firms as soon as possible.

Data protection

On 3 December 2020, the ICO held an informative webinar aimed at small to medium businesses on key data protection requirements to consider at the end of the transition period. Click [here](#) to watch.

If firms haven't done so already, it is recommended that they sign up to the [ICO's newsletter](#) to receive regular updates on data protection developments.

The UK has confirmed the position on data transferred from the UK to the EEA and there will be no changes to the way that personal data is sent to the EEA. However, what is yet to be confirmed is whether data can be transferred the other way e.g. EEA to the UK and the EU is yet to decide whether it accepts the UK's data protection regime as adequate. If the EU does grant positive data adequacy decisions by 1 January 2021 then it would mean that personal data can flow freely from the EEA to the UK, without any action by firms.

To mitigate the risks should data adequacy decisions not be granted in time, firms that receive data into the UK from the EEA should put in place alternative transfer mechanisms such as standard contractual clauses (SCC).

Please note, if a customer is sending you their own personal data then you do not need to use SCC's or any other transfer safeguard, as GDPR does not restrict transfers from the data subject themselves.

*European Economic Area. EEA includes EU countries and also Iceland, Liechtenstein and Norway.

The contents of this guidance do not constitute legal or other professional advice. Users should seek appropriate legal guidance before coming to any decision or either taking or refraining from taking any legal action. AMI disclaims all liability for loss and/or damage that may result from its use.

For member firms the use of SCC's may be necessary if data is processed, stored (e.g. on a cloud-based server) or outsourced (e.g. call centre) to the EEA and this data flows from the UK to the EEA and back again.

The ICO has created an [interactive tool](#) for small and medium-sized businesses based in the UK who need to maintain the free flow of personal data into the UK from Europe (should data adequacy not be granted before the end of the transition period).

Firms should check and understand how data is arranged and stored, for example where in the world is the data backed up? Firms should also make sure they understand where data is stored if using products such as Microsoft and Apple.

EU representatives

- **What are EU representatives?**

An EU representative acts as a point of contact for lead supervisory authorities and data subjects. They need to be established in an EEA member state where your data subjects are based.

The role of an EU representative includes acting on a firm's behalf in relation to EU GDPR compliance (including maintaining local records of processing) and dealing with any supervisory authorities or data subjects in this respect.

- **Is this relevant to my firm?**

[ICO guidance](#) goes into more detail on situations where this would apply. However, this will capture some member firms where goods or services are offered to individuals in the EEA. AMI's interpretation of this is that this would not capture the servicing of existing customers based in the EEA but rather new business where these services are being actively offered to EEA based customers. For example, where a firm offers and promotes mortgage services for expats located in the EEA.

The ICO guidance goes into more detail on the rules but the key points are that the EU representative must be someone based locally (i.e. where some of the individuals whose personal data you are processing in this way are located); can be an individual, company or organisation established in the EEA; and they must be able to represent you in relation to your obligations under the EU GDPR. Typically, this is likely to be a law firm, consultancy, or private company.

Documentation and privacy notices issued to EEA based customers should be updated to include details of the EU representative.

*European Economic Area. EEA includes EU countries and also Iceland, Liechtenstein and Norway.

The contents of this guidance do not constitute legal or other professional advice. Users should seek appropriate legal guidance before coming to any decision or either taking or refraining from taking any legal action. AMI disclaims all liability for loss and/or damage that may result from its use.

A summary of adequacy decisions, safeguards and exceptions as provided in the ICO webinar:

	Adequacy	Safeguards			Exceptions
		SCCs	BCRs	Other	
Sending data from the UK to EEA	Transfers to the EEA will not be restricted				
Receiving data into the UK from EEA	No adequacy so far	EU GDPR will continue to apply to an EEA sender of personal data. Understanding the sender's obligations and how you may assist them would be beneficial for the data flow between the organisations.			
Sending data from the UK outside EEA	Existing adequacy decisions will be recognised	Existing SCCs will be recognised. Organisation may need minor amendments to reflect that the SCCs apply to the UK rather than the EU	Existing EU BCRs need to be re-authorised by the ICO	Will apply in a similar way as under the EU GDPR	Will apply in the same way as under the EU GDPR
Receiving data into the UK from a non-EEA country	Specific arrangements are being worked on	It would be up to the sender to ensure that they are complying with the rules in their country. Upon receiving the personal data, the UK organisation would need to comply with the data protection rules in the UK, i.e. the UK GDPR			

Will the General Data Protection Regulation (GDPR), Privacy and Electronic Communications Regulations (PECR) and Data Protection Act (2018) continue to apply in the UK after the transition period?

- The GDPR will be converted into UK law so will continue to apply in the UK after the transition period. Firms should note that the EU version of the GDPR may also still apply directly if you operate in Europe, offer goods or services to individuals in Europe or monitor the behaviour of individuals in Europe.
- PECR (the rules that cover marketing, cookies and electronic communications) are set out in UK law so will also continue to apply at the end of the transition period.
- The Data Protection Act 2018 (DPA 2018) will continue to apply.

The ICO has produced an [FAQ](#) on information rights at the end of the transition period.

Firms should also review [government guidance](#) on using personal data in businesses from 1 January 2021 and [ICO guidance and resources](#) on data protection at the end of the transition period.

The ICO has created a [specific guide for SME businesses](#) which is likely to be most relevant to member firms.

Firms should ensure that they amend their privacy notices and documentation with reference to the applicable data protection legislation. For example, firms that deal with UK customers only will need to take out any reference to the EU GDPR and refer to the applicable UK legislation (this is primarily the UK Data Protection Act 2018). The EU GDPR will continue to apply to customers based in the EEA, so firms should make it clear which data protection regime applies in these circumstances.

Firms may also need to review their Data Protection Impact Assessment (DPIA).

*European Economic Area. EEA includes EU countries and also Iceland, Liechtenstein and Norway.

The contents of this guidance do not constitute legal or other professional advice. Users should seek appropriate legal guidance before coming to any decision or either taking or refraining from taking any legal action. AMI disclaims all liability for loss and/or damage that may result from its use.

Employing EU citizens in the UK

From 1 January 2021 the UK will introduce an immigration system and anyone that a firm wants to recruit from the outside the UK (excluding Irish citizens) will need to apply for permission first. Firms will need to have a sponsor licence to hire most workers from outside the UK.

The Home Office has provided information for employers on employing EU, EEA and Swiss citizens in the UK, covering right to work checks, the EU Settlement Scheme and the UK's new immigration system. This can be found [here](#).

Other considerations

- We are aware that some insurance providers have advised EEA based customers that they will need to change bank accounts to continue their insurance policies. This could result in commission clawback if protection policies of EEA based customers are cancelled.
- Businesses and consumers will no longer be able to use the Online Dispute Resolution (ODR) platform from 1 January 2021. The ODR platform is an EU website that links consumers with Alternative Dispute Resolution (ADR) providers in the EU. Firms should remove links and references to the ODR platform from their websites from 1 January 2021.
- We await confirmation from the FCA as to the FOS and FSCS rights of individuals that have UK property but reside in the EEA.
- If a firm has an Appointed Representative (AR) in an EEA country, then the principal firm would need to make sure that the AR meets the laws of that jurisdiction. The principal firm is also likely to need to be approved and regulated by the local regulator in that jurisdiction.

Useful links and information

- [FCA Brexit information hub](#)
- FCA dedicated Brexit helpline: 0800 048 4255
- [FCA Brexit videos](#)
- [HM Treasury financial services sector end of transition period guidance](#)
- [Government Brexit transition tool checker](#)
- [Providing services and travelling for business to the EU, Switzerland, Norway, Iceland and Liechtenstein: country guides](#)
- [ICO data protection guidance](#)
- ICO helpline: 0303 123 1113
- [Money Advice Service - banking, insurance and financial services changes after Brexit](#) (useful overview for consumers)

*European Economic Area. EEA includes EU countries and also Iceland, Liechtenstein and Norway.

The contents of this guidance do not constitute legal or other professional advice. Users should seek appropriate legal guidance before coming to any decision or either taking or refraining from taking any legal action. AMI disclaims all liability for loss and/or damage that may result from its use.