Brexit checklist

Last updated January 2019

Brexit will have a profound impact on the UK. Advising business how to navigate Brexit, as you may appreciate, is very challenging given the current uncertainty about the final outcome. However, we have developed this checklist to help members understand some of the key aspects of your business that Brexit may affect, particularly if you do business in the EU/EEA, and what you can do now to prepare for it. The checklist is not exhaustive, but it should be a good starting point from which to develop your plans (and contingency plans), and it incorporates some of the Information Commissioner's Office (ICO) "Leaving the EU – six steps to take" guidance which we also recommend reading in full.

We will update this checklist when more details of Brexit have been confirmed. In any case, we recommend that you seek legal advice or consult a tax advisor on any concerns about the specifics of your business when trading in the EU or EEA post-Brexit.

Please read our Brexit FAQs alongside this checklist which explain more about Brexit and help answer some of the most common questions, including what a 'no deal' scenario means for digital advertising. Whatever stage you are at in planning for Brexit, we are keen to hear how Brexit might impact your business, and if you have any questions that aren't covered in our FAQs or checklist. Email us on policy@iabuk.com.

Preparing for Brexit: 10 steps to take now

1. Make your organisation aware

It is important that the key people in your organisation are aware of the key issues concerning Brexit and are kept up-to-date with the latest information and guidance.

The UK Government has recently launched a website to help businesses to prepare for Brexit: https://euexitbusiness.campaign.gov.uk. It has also published detailed Brexit technical notices covering various aspects of Brexit, including data protection and the statutory instruments that will be in place in the event of a no-deal Brexit. These technical notices should also be read in conjunction with the EU's preparedness notices.

The ICO has published guidance for organisations on data protection and Brexit, which includes guidance on international data transfers in a 'no-deal' scenario.

We recommend that you bring together different departments to raise awareness across all aspects of your business and draw up contingency plans for a no-deal scenario that involve members of staff from all relevant departments.

2. Review business plans

Most economic forecasts appear to be predicting that the UK will suffer an economic downtown following Brexit, although there is a debate about what the extent of any impact might be. Even with the best forecasts, it is notoriously difficult to predict actual outcomes, but there is already evidence that the current uncertainty is feeding into the wider economy. This will no doubt have an effect on Sterling/Euro and Sterling/US Dollar exchange rates and exposure to currency volatility could affect your business plans and revenue targets.

3. Audit your contracts

We recommend that you conduct an audit of your contracts with EU/EEA based customers. Will your contract with an EU/EEA based client require renegotiation or termination as a result of Brexit? Does your contract have territorial references to the EU/EEA? If you may want to clarify if this will cover the UK, post-Brexit.

As mentioned above, contracts denominated in currencies other than Sterling will expose to you to currency risk.

If your contract requires personnel to travel between the UK and EU or EEA Member States to deliver services, you will need to consider how this will be affected by Brexit. In the absence of an agreement post-Brexit, the UK will be treated like a third country. This means that UK companies or independent professionals providing services into an EU or EEA Member State, through the temporary movement of people i.e. consultants, secondments, intra-group transferees, etc. may be subject to a local economic needs test.

4. Signpost your EU workers to information on the EU Settlement Scheme

If you have UK-based EU workers in your organisation, it may be helpful to signpost those staff to information on how to apply for the EU Settlement scheme if they wish to stay in the UK with their families beyond 30 June 2021. At the moment this scheme does not apply to non-EU EEA Member States (Iceland, Liechtenstein and Norway) and Switzerland. But the UK is looking to secure a similar deal and talks are ongoing.

EU citizens and their families who are resident in the UK before the end of the implementation period ('transition period') on 31 December 2020 will be able to apply for the EU Settlement Scheme to continue living in the UK after 30 June 2021. (n.b. these dates are subject to change in the event of a 'no deal' Brexit). Successful applicants will receive settled or pre-settled status depending on the length of time spent in the UK prior to application. Applicants will need a valid passport and provide evidence of living in the UK. The Home Office has introduced technology to help speed up the process with the ability to use a smart phone (Android only) to read a biometric passport, and it will be possible to apply online. The scheme is being phased in and will be fully open by 30 March 2019, with deadline for applications on 30 June 2021. Detailed guidance can be found on the UK Government website.

The Home Office has published an employer toolkit to equip employers with the right tools and information to support your EU staff.

5. Review future workforce plans and conduct risk analysis

The Government has recently published its White Paper on Migration which sets out its plans to introduce a new single immigration system, ending free movement, but it may be some time before policy or legislation is enacted. In the meantime, it will be important to conduct a detail workforce risk analysis. It is likely that there will be a greater rate of attrition for EU/EEA citizens working in the UK if they stay for shorter amounts of time than in the past. It appears that the future migration system, while not confirmed, will mean that EU/EEA nationals are not be treated any differently (i.e. not preferentially) to non-EU/EEA nationals and so EU/EEA workers may be harder to replace than currently. This may lead to increased pressure on wage costs due to labour shortages and higher inflation.

6. Continue to comply with GDPR

The Data Protection Act 2018 will remain in place and the Government will incorporate GDPR directly into UK law after Brexit. This means you should continue to implement GDPR compliance standards and follow current ICO guidance.

7. Review your data transfers to and from the EU/EEA

The UK has stated that it will continue to allow data transfers to the EU/EEA even after Brexit. However, the EU Commission needs to grant data adequacy status to allow the free flow of data to the UK as a third country. In the absence of a data adequacy decision, you may want to consider putting standard contractual clauses (SCC) in place as a contingency measure. Setting up SCCs may have additional associated

costs. However, the ICO has developed an online tool for SMEs which will automatically generate approved model SCCs. These can then be adapted to your own individual business requirements.

If you are a multinational group with existing binding corporate rules (BCRs) that cover the EU/EEA and UK group companies, with appropriate changes to show the new status of the UK as a third country, these BCRs are likely to permit the transfer from the EU/EEA to the UK. This is subject to confirmation from the European Data Protection Board (EDPB).

8. Review your European operations for GDPR compliance

Under the GDPR, if you are based in the UK, and not in any other EU or EEA state, but you offer goods or services to individuals in the EU/EEA, or you monitor the behaviour of individuals located in the EU/EEA, then to comply with legislation you will need to appoint a suitable representative in the EU/EEA. This is separate from your Data Protection Officer (DPO) obligations. The data protection representative is responsible for liaising with data protection authorities in the EU and EEA Member States.

If the UK is currently your lead supervisory authority, you should review the structure of your European operations to assess whether you will continue to be able to have a lead authority within the EU/EEA and benefit from the one-stop-shop. The one-stop-shop means you can generally deal with a single European data protection authority acting on behalf of the other European supervisory authorities. It avoids having to deal with regulatory and enforcement action from every supervisory authority in every EU and EEA state where individuals are affected.

However, the GDPR's cooperation and consistency mechanism only applies to controllers with an establishment, or establishments, within the EU/EEA. Assuming that the UK will be treated like a third country after Brexit, if your company does not have an establishment in the EU/EEA, the European Data Protection Board (EDPB) has said that the mere presence of a representative in an EU/EEA Member State does not trigger the one-stop-shop system. This means that controllers without any establishment in the EU/EEA must deal with local data protection authorities in every EU and EEA Member State they are active in, through their local representative.

9. Review your data transfers from the UK to non-EU/EEA countries

The UK Government has said it plans to recognise adequacy decisions made by the European Commission prior to Brexit as part of the UK's own data protection framework. This will allow restricted transfers to continue to be made to those organisations, countries, territories or sectors covered by an adequacy decision.

If you want to make a restricted transfer to a country that currently is not covered by an adequacy decision, you will need to make arrangements to put in place one of the listed appropriate safeguards. For most businesses an SCC might make the best option.

If the UK exits the EU without a deal, members wishing to continue to make data transfers to US organisations under the EU/US Privacy Shield will need to check that the US organisation has made the necessary update to its commitment to compliance with the Privacy Shield. Confirmation of the update should usually be possible by checking the US organisation's publicly available privacy policy. The US government's Privacy Shield website has information for US Privacy Shield participants on what they should do to continue receiving personal data from the UK.

10. Audit personal data stores

Does the personal data you currently store easily distinguish between UK citizens' and EU/EEA citizens' data? Given that the UK plans to have its own data protection framework, you may consider segregating your data to provide flexibility in case of future regulatory changes.