ICAEW KNOW-HOW
TECHNICAL STRATEGY DEPARTMENT
BREXIT GUIDE

DATA PROTECTION AND BREXIT

Issued December 2018
Updated October 2020

October 2020 Update on Data Protection and Brexit – what you need to know and how to prepare your business

This guide is part of a series that explains some of the issues surrounding Brexit. It is intended to provide practical information to ICAEW members. It is not intended to constitute legal advice. If in doubt, members are advised to seek independent legal advice.

Following the agreement (in principle) of a Brexit withdrawal agreement (or 'deal') with the EU, the UK left the EU on 31 January 2020. Since then the UK has been in a transition period. This will end on 31 December 2020.

During the transition period the rules on data protection are as before but once the transition period ends this will no longer be the case. This guide explains what you need to do to prepare your business to ensure the free flow of personal data after the transition period has ended and until an adequacy decision has been agreed.

Action will be required if:

1. You wish to continue the transfer of the personal data of EU data subjects from the EEA to the UK
2. You wish to process the personal data of EU data subjects but you do not have an establishment in the EU.

In addition and if neither of the above apply:

1. You must continue to comply with the relevant UK data protection legislation.
2. You may have to update your documentation to refer to UK legislation in effect after 1 January 2021.

Introduction

The General Data Protection Regulation (GDPR) co-ordinates data protection law across the European Union (EU). This is to facilitate the free flow of personal data and to protect the rights of EU data subjects whose personal data is transferred to countries outside the EU. Countries outside the European Economic Area (EEA) are deemed 'third countries' and organisations or individuals within a third country cannot assume that they can automatically transfer or process the personal data of EU data subjects.

When the UK leaves the EU it will become a third country. This means UK organisations and individuals that process or transfer the personal data of EU citizens from the EU to the UK may need to take action to continue the free flow of data from the EU to the UK and the protection of EU data subjects.

Why could Brexit impact the transfer of personal data?

Once the UK leaves the EU it will be deemed a third country. Under the GDPR, as before, any third country to which the personal data of EU data subjects is transferred must have in place a data protection regime considered to be equivalent to EU legislation. To prove this the EU Commission can issue what is known as an 'adequacy decision'. There are a number of other GDPR-compliant ways to transfer data from the EU to countries outside the EU if no adequacy decision is in place but all of these involve action being taken by organisations and individuals to demonstrate that the transfer is GDPR-compliant. In other words, you cannot just assume that you are allowed to transfer the personal data of EU data subjects out of the EEA. If you do when you shouldn't, you may be fined and/or face other sanctions

Why could Brexit impact the processing of the personal data of EU data subjects?

For personal data transfers from the EU to the UK – action required:

Post-Brexit, the UK will be deemed a third country and so EU organisations will only be able to transfer personal data from the EU to the UK if there is an adequacy decision or some other arrangement in place.

The exact nature of arrangements that will be in place after Brexit will depend on whether there is a deal or not (see below) and how long it takes for the EU to agree an adequacy decision.

Any UK organization receiving personal data from an organization in the EEA cannot assume, therefore, that such transfers can continue as now, that is before an adequacy decision has been made or without putting in place alternative arrangements.

For personal data transfers from the UK to the EU – no action required:

Brexit will have less impact as the Data Protection Act 2018 (DPA 2018) will still be the applicable legislation. The GDPR, however, will be retained in UK law under the terms of the EU (Withdrawal) Act 2018 (EUWA 2018).

The UK government could of course decide in future that further protections are needed for UK data subjects and restrict transfers from the UK but that seems unlikely, at least in the short term.

EU data subjects – possible action required:

The GDPR requires a controller or processor not established in the EEA (so this will include any controller or processor only established in the UK post Brexit) to designate a representative within the EEA if they process the personal data of EU data subjects. This includes offering goods or services to individuals in the EEA and/or monitoring the behaviour of individuals located in the EEA. This does not apply to public authorities or if the processing is occasional, low risk and not special category or criminal offence data.

What are the implications of the Withdrawal Agreement?

Under the terms of the Withdrawal Agreement:

1. The EU Commission will begin its assessment of the UK's data protection regime once the UK leaves the EU. Assuming a full adequacy decision is made, then UK organisations and individuals will not need to take any further steps. If no adequacy decision or only a partial one is made, UK organisations and individuals must adopt other measures (see below) to continue processing and transferring the personal data of EU data subjects from the EU to the UK.

2. The transition period after the UK leaves the EU will last until 31 December 2020.
3. In the transition period:
    a. All EU privacy laws such as the GDPR and the ePrivacy Directive will continue to apply in the UK.
    b. As mentioned above, the EU Commission will begin its assessment of the UK's data protection regime with the aim of adopting an adequacy decision by the end of 2020.
    c. The UK's data protection authority (the ICO) will cease to participate in the European Data Protection Board (EDPB) and will only have 'observer' status. The EDPB issues guidance and oversees the enforcement of the GDPR including the one-stop shop mechanism of regulatory oversight.
    d. The Court of Justice of the European Union (CJEU) will continue to have jurisdiction over questions of interpretation raised by UK courts regarding data protection law during the transition period.

What if there is 'no deal'?

The government has confirmed that if there is a no-deal Brexit it will make a number of changes to the DPA 2018 using the regulation-making powers given under the EUWA 2018. This is to ensure that the existing data protection framework will continue to operate effectively once the UK is a third country.

This means that:

1. The EU GDPR standards will be preserved in UK law.
2. All the EEA countries will be recognised as 'adequate' and so data flows from the UK to the EEA will continue **BUT** the UK government cannot legislate to allow the free flow of data into the UK. This means alternative mechanisms for the transfer of personal data from the EU to the UK will need to be put in place by UK organisations and individuals unless and until an adequacy decision is made by the EU.
3. Existing EU adequacy decisions for countries outside of the EU will be preserved on a transitional basis. This means UK organisations can continue to rely them.
4. EU standard contractual clauses (SCCs) will be recognised in UK law and the ICO will be given the power to issue new clauses.
5. Any binding corporate rules (BCRs) authorised before the UK leaves the EU will continue to be recognised. After that date the ICO will continue to authorise new BCRs under UK law.
6. The extraterritorial scope of the UK data protection framework will be maintained. This means that data controllers or data processors not based in the UK but who process the personal data of individuals (data subjects) in the UK will be subject to the UK's data protection legislation. This will include data controllers or data processors based in the EU if they process the personal data of UK data subjects post Brexit.
7. Non-UK data controllers subject to the UK data protection framework will have to appoint representatives in the UK if they are processing UK data on a large scale.
8. If you are based in the UK but not in the EEA and offer goods and/or services to individuals in the EEA or you monitor the behavior of individuals located in the EEA you will need to appoint a representative based in the EEA. This representative will act as the contact with individuals and data protection authorities. It cannot be your Data Protection Officer or one of your processors. This will not be necessary if you are a public authority or the processing is occasional, low risk and does not involve special category or criminal offence data on a large scale.

What are adequacy decisions?

As noted above the government has assumed that the EU will issue an adequacy decision, but what is an adequacy decision? In simple terms it is an acknowledgement by the EU (or by proof) that the data protection regime in a third country offers the same level of protection to EU data subjects as EU legislation. That being so the transfer of personal data of EU data subjects to that third country is permitted, although it still must be GDPR-compliant.

There are two types – full and partial:

a. Full

A full adequacy decision means that there are no restrictions on the transfer of personal data to these countries. In this case all an EU organisation needs to do is check that the country to which it wishes to transfer personal data has a full adequacy decision.

So far 12 countries including Japan, Switzerland, Argentina and New Zealand have successfully negotiated a full adequacy decision. Negotiations are ongoing with a number of other countries including South Korea but it can be a very lengthy process (years rather than days).

Adequacy decisions are subject to review by the EU Commission and so can be amended or revoked at any time.

b. Partial

Canada and the US have only been granted 'partial' adequacy decisions. This means not all organisations and not all types of personal data are covered by the decision.

1. The Canadian adequacy decision only covers data that is subject to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA). Not all data is subject to PIPEDA.
2. The EU–US Privacy Shield framework allowed the transfer of personal data from the EU to the US if a US-based organisations self-certified to the US Department of Commerce that they comply with the Privacy Shield Principles. See the US Department of Commerce's Privacy Shield and the UK FAQs

July 2020 Update: the CJEU ruled on 16 July 2020 that the EU-US Privacy Shield was invalid, with immediate effect. This means additional alternative mechanisms must be put in place (such as SCCs) for the transfer of personal data from the EU (including from the UK before the end of the transition period) to the US. The ICO has said it will take a pragmatic approach but has provided no specific guidance on what organisations should do. See here for the ICO's latest statement.

What if there is no adequacy decision between the UK and the EU post Brexit?

Clearly a full adequacy decision permitting the transfer of all personal data from the EU to the UK post-Brexit is the most desirable outcome. But if there is no such decision, there are a number of alternative mechanisms available that offer 'appropriate safeguards' over the personal data of EU data subjects. These only apply in specific situations and are subject to very strict rules.

a. Binding corporate rules (BCRs) can be used by multinational organisations when transferring personal information outside the EEA but within their group of entities and subsidiaries. Organisations must get approval for their BCRs from an EU data protection authority, with one authority acting as the lead. The EDPB has issued guidance on using BCRs post Brexit.

b. The use of EU Commission-approved 'standard contractual clauses' (SCCs) (also known as model clauses as set out in the annex to EU decision 2010/87/EU) within a contract.

The clauses contain contractual obligations on both the data exporter (based inside the EEA) and the data importer (based outside the EEA) and rights for the individuals whose personal data is transferred. Individuals can directly enforce those rights against the data importer and the data exporter. SCCs are probably the best bet for most organisations, but even so the model clauses run to nine pages and businesses should seek their own legal advice before seeking to rely on them.

c. The GDPR has eight permitted exceptions but these should only be used as true 'exceptions' from the general rule that you should not make a transfer unless it is covered by an adequacy decision or there are appropriate safeguards in place. In most cases they can only apply to 'occasional' and 'necessary' transfers or in very specific one-off instances (such as to protect the vital interests of a data subject in a medical emergency). Some permitted exceptions require you to inform and justify your actions to the ICO before you make the transfer. As the permitted exceptions are so narrow in scope they are unlikely to be of use in the majority of cases.

The GDPR has also introduced two new options. Neither are fully in place yet, but it is possible that if they are implemented before Brexit they might offer a more practical alternative to the three mechanisms above. These are:

a. *Codes of conduct* – The code of conduct must be approved by a supervisory authority and include appropriate safeguards to protect the rights of individuals whose personal data is transferred, and which can be directly enforced and monitored.

b. *Certification schemes* – These must be approved by a supervisory authority and include appropriate safeguards to protect the rights of individuals whose personal data is being transferred, and which can be directly enforced.

What if there is no adequacy decision between the UK and the EU post Brexit?

The government is advising that organisations should 'proactively' consider how they will ensure the continued free flow of data from the EU to the UK.

Remember this only applies to transfers from the EU to the UK. Transfers from the UK to the EU will continue to be subject to the DPA 2018 and so you must continue to ensure that you are compliant with current UK legislation.

There is no guarantee that an adequacy decision will be approved before the end of the transition period or that it will be a full adequacy decision, although the government is confident that a full adequacy decision will be made.

We advise that the following actions should be taken as soon as possible and certainly before the end of the transition period (31 December 2020).

1. Sign up to receive alerts from the ICO and the Government .The situation is changing all the time and this is the best way to ensure you remain compliant.
2. Review your personal data flows:

- Check if any of the personal data that you currently process is transferred from the EEA to the UK. If it is, set up the appropriate, or have plans in place to set up, the appropriate alternative data protection mechanism (see above), should you need or wish to continue processing this personal data if there is a no-deal Brexit or if no adequacy decision is agreed.
- Take stock of personal data you hold so that you can distinguish between data acquired before the end of the transition period and after. This is because organisations in the UK will need to comply with EU data protection law (as it stands on 31 December 2020) when processing personal data that was gathered before the end of the transition period and relates to individuals who live outside the UK.
- For any personal data currently transferred from the UK to outside the EEA, you

should already have in place GDPR-compliant mechanisms. You will still need these post Brexit so check that you have the correct mechanism in place.

- Don't forget to check where any of your IT service providers process data – many cloud storage providers, for example, process data outside of the EEA. Ask what steps they have taken to ensure they can continue to process personal data post Brexit.

3. Check if you need to appoint a lead supervisory authority in an EU member state
   - Check if you process the personal data of EU data subjects and have the ICO as your lead supervisory authority, under the 'one-stop shop' principle. Post Brexit this will not be possible and you will need to appoint a lead supervisory authority in an EU member state. This can either be in an EU country where you have an 'establishment' (eg a subsidiary or group company) or in the EU country where the data subjects, whose data is being processed by you, live.
4. Review and update documentation
   - All documentation including privacy notices will require the removal of any reference to EU law or EU terminology and changed to reflect UK terminology and safeguards.
   - If you intend to rely on the US Privacy Shield after the transition period (and the government has indicated that this will be possible) ensure the US organisation has changed its documentation to refer to UK law
5. Contact the ICO – if you have specific questions call 0303 123 1113
6. If in doubt, seek legal advice.

Want to know more?

1. For more detailed advice from the ICO read:
   - Guide to International transfers under the GDPR
   - Guide to Brexit and the Transition period.
2. Sign up to receive the ICO's newsletter on the latest developments and what to do next.
3. Use the ICO's interactive tool for SMEs to check whether you need to set up standard contractual clauses and if so, how to do this.
4. For more Brexit support, visit ICAEW's Brexit hub
5. For the government's latest advice
   - On a no-deal Brexit see here
   - Sign up to receive alerts from the government on the transition period
   - On using personal data after Brexit see here
6. For the current Withdrawal Agreement see here

CONTACT US

mail to: brexitsupport@icaew.com

europe@icaew.com

Chartered accountants are talented, ethical and committed professionals. There are more than 1.8m chartered accountants and students around the world, and more than 186,500 of them are members and students of ICAEW.

ICAEW promotes inclusivity, diversity and fairness. We attract talented individuals and give them the skills and values they need to build resilient businesses, economies and societies, while ensuring our planet's resources are managed sustainably.

Founded in 1880, we have a long history of serving the public interest and we continue to work with governments, regulators and business leaders around the world. We are proud to be part of Chartered Accountants Worldwide, a global network of 750,000 members across 190 countries, which promotes the expertise and skills of chartered accountants on a global basis.

We believe that chartered accountancy can be a force for positive change. By sharing our insight, expertise and understanding we can help to create strong economies and a sustainable future for all.

www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com/

T +44 (0)20 7920 8646
E brexitsupport@icaew.com