ICAEW KNOW-HOW
TECHNICAL STRATEGY DEPARTMENT
BREXIT GUIDE

DATA PROTECTION AND BREXIT – UPDATE

September 2019

Brexit and data protection – what you need to know and how to prepare your business.

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 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 (now set for 31 October 2019) 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 protection of EU data subjects.

The action required will vary according to whether there is a deal (as set out in any withdrawal agreement) or no deal.

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?

UK businesses currently benefit from the 'one-stop shop' principle. This allows a single data protection authority (such as the Information Commissioner's Office (ICO) in the UK) to be the lead supervisory authority for organisations carrying out cross-border processing. For an organisation in a third country (such as the UK, post Brexit) to benefit from the one-stop shop principle, it will need to appoint a lead supervisory authority in an EU member state but only if it can show it has a main 'Establishment' there; this could be a subsidiary or other group company. If there is no

Establishment within an EU state then they will have to appoint a representative in the state where the data subjects, whose data is being processed, live.

What does this mean for the UK after Brexit?

For personal data transfers from the EU to the UK:

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 EU has confirmed that it will not begin the process to agree an adequacy decision until after the UK has left the EU. Furthermore, 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.

For personal data transfers from the UK to the EU:

Brexit will have less impact as the Data Protection Act 2018 (DPA 2018) will still be 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.

For the processing of the personal data of EU data subjects:

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 behavior of individuals located in the EEA. This does not apply to public authorities or if the processioning is occasional, low risk and not special category or criminal offence data.

September 2019 update – What will happen if there is a deal?

The Withdrawal Agreement (or 'deal') negotiated by Theresa May in 2018 has now been rejected by Parliament. The current government has said it is committed to negotiating a new deal. It seems likely that with regard to Data Protection any new deal will be substantially the same as the previous deal.

The following is based on the previous deal (Withdrawal Agreement) and is given as guide as to what may happen. We will update this once we know more.

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. Any Withdrawal Agreement is likely to include a transition period after the UK leaves the EU. The length of any such transition deal is currently unknown.
3. In any 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.

September 2019 update – what if there is 'no deal'?

The government has confirmed that if there is a no-deal Brexit (see 23 April 2019 guidance), it will make a number of changes to the DPA 2018 using the regulation-making powers given under the EUWA. 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 of 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 on the Privacy Shield if, for example, they wish to transfer personal data from the UK to the US. But UK organisations must check that the US organization to which they are transferring data has amended its terms and conditions (including privacy notices) to include reference to both the UK and the EU.
4. EU standard contractual clauses 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.
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 10 countries including Switzerland, Argentina and New Zealand have successfully negotiated a full adequacy decision. Negotiations are ongoing with a number of other countries including Japan and 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 allows the transfer of personal data from the EU to the US:
   - Applies only to those US-based organisations that have self-certified to the US Department of Commerce that they comply with the Privacy Shield Principles. Any EU organisation that wishes to transfer personal data to a US organisation under the Privacy Shield must check the Privacy Shield list to see whether the organisation concerned has signed up.
   - Any US organization signing up to the Privacy Shield must amend its terms and conditions (including its privacy notices) to include reference to the UK and to the EU. It will be responsibility of the UK organisation to check that this has been done before the Brexit date if there is no deal. See the US Department of Commerce's Privacy Shield and the UK FAQs

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.

b. The use of EU Commission-approved 'standard contractual clauses' (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 the data exporter (i.e., an organisation based outside the EEA) and the data importer (based inside 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. However, the model clauses run to nine pages and businesses may wish to obtain 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. The EDPB is currently drafting guidelines on codes of conduct as appropriate safeguards for international transfers.

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. The EDPB is currently drafting guidelines on certification as an appropriate safeguard for international transfers.

What can I do now to ensure my business will comply with data protection regulations 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 if there is a no-deal Brexit. 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 should continue to ensure that you are compliant with current UK legislation.

Even if there is a deal that comes into effect post- Brexit, there is no guarantee that an adequacy decision will be approved before the end of any transition period or that it will be a full adequacy decision.

We advise the following actions should be taken as soon as possible and before Brexit if there is no deal:

- Check if any of the personal data that you currently process is transferred from the EEA to the UK, and set up the appropriate, or have plans in place to set up, the alternative data protection mechanisms that are available (see above), should you need to use one of these if there is a no-deal Brexit or if no adequacy decision is agreed.
- 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.
- 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.
- Review your documentation – including Privacy Notices, Letters of Engagement - for any reference to EU law or EU terminology and change this to reflect UK terminology.
- If you rely on the EU-US Privacy Shield check that the US organization to whom you transfer data has signed up to and complied with the requirements of the Privacy Shield and has amended its documentation to refer to both the UK and the EU.
- If in doubt, seek legal advice.

How do I find out more?

- For more detailed advice read the ICO's guidance to international transfers under the GDPR and its guide to Brexit
- The ICO has set up an interactive tool to be used by SMEs to check whether they need to set up standard contractual clauses and if so, how to do this.
- For more Brexit support, visit ICAEW's Brexit hub
- For the government's latest advice (as at **23 April 2019**) on a no-deal Brexit see here
- For the previous Withdrawal Agreement see here

CONTACT US

mail to: brexitsupport@icaew.com

europe@icaew.com

ICAEW is a world leading professional membership organisation that promotes, develops and supports over 150,000 chartered accountants worldwide. We provide qualifications and professional development, share our knowledge, insight and technical expertise, and protect the quality and integrity of the accountancy and finance profession.

As leaders in accountancy, finance and business our members have the knowledge, skills and commitment to maintain the highest professional standards and integrity. Together we contribute to the success of individuals, organisations, communities and economies around the world.

Because of us, people can do business with confidence.

ICAEW is a founder member of Chartered Accountants Worldwide and the Global Accounting Alliance.
www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com.

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

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