Birketts

Brexit and GDPR: what you need to know and do

Kitty Rosser
Senior Associate
01603 756559
kitty-rosser@birketts.co.uk

Introduction

Many organisations have yet to update their GDPR procedures for Brexit. Whilst the justifications for this are many and varied, one consistent message we are hearing is that organisations simply do not know what is required of them. This is perhaps unsurprising given that, as with so many aspects of data protection, there is no one size fits all solution. The situation is, of course, not helped by the ongoing uncertainty as to whether and when the UK will actually exit the EU and the terms of the deal, if any, under which it will leave.

This guide is intended to assist organisations to understand the issues and identify what actions they may need to take. It includes a summary of the headline issues and terms that organisations planning for Brexit need to be aware of together with a practical checklist to help organisations identify what compliance steps they will need to take.

In brief

1. Many organisations will need to update their data protection compliance measures for Brexit.
2. It is important that you familiarise yourself with the issues that Brexit poses for GDPR compliance now. These are summarised in the Headline Issues section of this guide. It will take you less than 10 minutes to read.
3. Use the Checklist section of our guide to identify what changes you need to make to prepare for Brexit.
4. If the UK exits the EU without a deal in place, you will need to have implemented the changes by exit day.
5. If the UK exits the EU with a deal in place you will have a little more time to make changes and the specific changes required may vary slightly. Look out for updated guidance from Birketts.

Click here to register for our corporate updates to ensure you receive updated guidance on GDPR and Brexit from Birketts.

Headline issues to be aware of

What is the 'UK GDPR'?

The GDPR is an EU regulation which means that it became law in the UK without the need for a UK Act of Parliament. When the UK exits the EU the GDPR will therefore no longer be law in the UK. However, if we leave without a deal the UK government intends to adopt the GDPR into UK law. A small number of necessary changes will be made to ensure that the law works in the UK and the law will be known as the 'UK GDPR'. It will sit alongside an amended version of the Data Protection Act 2018. If we exit with a deal in place, the GDPR will continue to apply until the end of the transition period.

What is the EEA?

The European Economic Area (EEA) was established by the EEA Agreement in 1992 and enables the extension of the EU's single market to non-EU member states. The EEA comprises all member states of the EU together with Norway, Liechtenstein and Iceland.

What is an adequacy decision and why does it matter?

Under the GDPR there is a general restriction on transferring personal data to countries outside of the EEA ('third countries'). Once we leave the EU, the UK will become a third country meaning that transfers of personal data to the UK from EEA states will be restricted. The EU Commission can issue adequacy decisions formally recognising that a third country's data protection laws offer an equivalent level of protection to data subjects as that existing under EU law. Where an adequacy decision has been issued personal data may be freely transferred from the EEA to the third country which is subject to that adequacy decision. The UK intends to seek an adequacy decision once we exit the EU to ensure that countries in the EEA can continue to transfer personal data to the UK freely. However, adequacy decisions take time and it is unlikely that the UK would be able to secure a decision within the first 12 months of exit. If we exit with a deal in place it may be possible to secure an adequacy decision before the transition period expires.

Can we still rely on Privacy Shield for transfers to the US?

The USA was unable to secure an adequacy decision from the EU Commission. Instead, the EU-US Privacy Shield was designed by the US Department of Commerce and the EU Commission to provide a mechanism to enable transfers of personal data from the EU to the US. The scheme is voluntary and US based organisations join by a process of self-certification and publicly committing to complying with the Privacy Shield requirements. Once an organisation has joined the Privacy Shield, the compliance commitment it makes becomes enforceable under US law. Once the UK leaves the EU, UK organisations will only be able to rely on the Privacy Shield to send personal data to a US recipient if that recipient has updated its Privacy Shield notices to say that it will apply the Privacy Shield commitments to both EU and UK personal data.

How do Standard Contractual Clauses (SCCs) work?

An organisation can overcome the general restriction on transferring personal data to third countries by implementing one of the several appropriate safeguards recognised under the GDPR. The most commonly used of these is the SCCs. These standard form contractual clauses were produced by the EU Commission and may be entered into between a data controller in the EEA acting as data exporter and a data controller or a data processor in a third country acting as data importer. SCCs cannot be used where data is being transferred between a data processor in the EEA and a data controller in a third country or where a transfer is made between two data processors. SCCs can be used alongside commercial contract terms but should be used in their complete and unedited form as deletions or amendments may cause the clauses to become invalid. There are several versions of the SCCs and care needs to be taken to ensure that the correct version of the SCCs is used. The Information Commissioner's Office ("ICO") has produced a useful tool to enable organisations to quickly and easily prepare appropriate SCCs. This can be found on the ICO's website at www.ico.org.uk

What is the UK Supervisory Authority?

Under the GDPR each member state of the European Union must appoint a regulator responsible for overseeing compliance with the GDPR and taking enforcement action where necessary. This regulator is known as the Supervisory Authority. The UK Supervisory Authority is the ICO. Post-Brexit the ICO will continue to be the regulator for UK data protection legislation but will cease to have standing as a Supervisory Authority under the GDPR. If we leave the EU without a deal, this change will happen immediately. If we leave with a deal in place, the ICO will retain its standing as a Supervisory Authority until the end of the transition period.

Will the one stop shop still apply?

Where an organisation either has offices, branches or other establishments in multiple EEA states, or has offices, branches or establishments in one EEA state only but undertakes processing activities that are likely to substantially affect individuals in one or more other EEA states, it is said to be engaged in cross-border processing. Under the GDPR's one stop shop provisions an organisation engaged in cross boarder processing deals with a single lead Supervisory Authority, which is responsible for regulating the organisation's cross-border processing and enforcing the GDPR (including issuing fines) on behalf of all other interested EEA Supervisory Authorities. This means that if the organisation's cross-border processing breaches the GDPR it is only investigated by one Supervisory Authority and only receives one fine across the EEA. Once the UK leaves the EU, UK organisations will deal with the UK ICO in respect of their UK activities but will deal with one or more other Supervisory Authorities in respect of their activities in the EEA. In the event of breach they may face enforcement action and fines from multiple Supervisory Authorities.

Will there be a transition period?

If the UK leaves the EU with a deal in place we will enter into a transition period. This will last until at least 31 December 2020 and may be extended up to 31 December 2022. For so long as the transition period continues, the GDPR will continue to take effect as UK law and the ICO will retain its status as a supervisory authority. During the transition period, it will be business as usual from a data protection perspective. If we leave without a deal in place there will be no transition period and the changes outlined in this guide will take immediate effect on exit day.

The checklist

Use the checklist below to work out which issues are relevant to your organisation and what action you need to take to ensure your GDPR compliance regime is ready for Brexit.

Work through each of the 7 questions in the checklist in turn. Look out for reminders and action boxes as you work through the checklist.

Checklist completed by:

Name:

Position:

Date:

Notes:

1. Can I continue sending personal data to the EEA?

A. Is this relevant to me?

☐ NO – I do not transfer personal data to other EEA states **(proceed to question 2)**

☐ YES – I do transfer personal data to other EEA states **(complete part B)**

B. Do I need to take any action?

☐ NO – the UK government has stated that transfers of personal data from the UK to EEA states will still be permitted after Brexit. No further action is required **(proceed to question 2)**

2. Can I continue sending personal data to third countries?

A. Is this relevant to me?

☐ NO: I do not transfer personal data to third countries **(proceed to question 3)**

☐ YES: I do transfer personal data third countries **(complete part B)**

Remember!

If you are sending personal data to another company this is still a restricted transfer even if the other company is part of the same corporate group as you.

Essential knowledge!
The countries which are currently subject to a full adequacy decision are Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Partial adequacy decisions have been in respect of Japan and Canada. The adequacy decisions for Japan only cover private sector organisations. The adequacy finding for Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Data Act. If you wish to transfer personal data to Japan or Canada you should seek specific legal advice as to whether you can rely on the partial adequacy decision.

B. Do I need to take any action?

☐ NO: **(if you only tick boxes in this section proceed straight to question 3)**

- ☐ I am only sending personal data to one or more third countries that are subject to an adequacy decision and I can continue to do this without taking any further action

AND/OR

- ☐ I am sending personal data to a third country which is not subject to an adequacy decision but I have already put SCCs or other appropriate safeguards listed in the GDPR in place

AND/OR

- ☐ I am sending personal data to a third country which is not subject to an adequacy decision and I have not put appropriate safeguards in place but I am relying on a derogation under Article 49 of the GDPR and can continue to do this without taking any further action

☐ YES: **(if you tick any boxes in this section you will need to take the action described in the relevant ACTION box. Make a note of this before you proceed to question 3)**

☐ I am sending personal data to a third country which is not covered by an adequacy decision or derogation under Article 49 of the GDPR and I have not yet entered into SCCs with the recipient or put any of the other appropriate safeguards listed in the GDPR in place

ACTION: Use the ICO's interactive tool "Keep data flowing from the EEA to the UK" to prepare the appropriate SCCs or identify an alternative appropriate safeguard. The tool is available on the ICO's website at www.ico.org.uk. If you wish to use SCCs you will need to send these across to the other party to sign. Make sure you allow time for this.

AND/OR

☐ I am sending personal data to a US recipient that is registered under the Privacy Shield

ACTION: Check that the recipient has updated its Privacy Shield privacy policy to specifically reference UK personal data. You can locate this via the Privacy Shield website at www.privacyshield.gov. If the US-based recipient hasn't already updated its privacy policy, you should contact it to explain that it will need to do so as soon as possible.

3. Can I continue receiving personal data from the EEA?

A. Is this relevant to me?

☐ NO: I do not receive personal data from other EEA states **(proceed to question 4)**

☐ YES: I do receive personal data from other EEA states **(complete part B)**

Remember!

If you are receiving personal data from another company this is still a restricted transfer even if the other company is part of the same corporate group as you.

B. Do I need to take any action?

☐ NO: I have already put SCCs or another appropriate safeguard listed in the GDPR in place **(proceed to question 4)**

☐ YES: I have not yet put SCCs or another appropriate safeguard listed in the GDPR in place **(you need to take the action described in the below ACTION box. Make a note of this before you proceed to question 4)**

> ***ACTION:*** **Use the ICO's interactive tool "Keep data flowing from the EEA to the UK" to prepare the appropriate SCCs or identify an alternative appropriate safeguard. The tool is available on the ICO's website at www.ico.org.uk. If you wish to use SCCs you will need to end these across to the other party to sign. Make sure you allow time for this.**

4. Can I continue receiving personal data from third countries?

A. Is this relevant to me?

☐ NO: I do not receive personal data from third countries **(proceed to question 5)**

☐ YES: I do receive personal data from third countries **(complete part B)**

Remember!

You still need to consider these rules even if you are receiving personal data from another company that is part of the same corporate group as you.

Essential knowledge!
The countries which are currently subject to a full adequacy decision are Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. Partial adequacy decisions have been in respect of Japan and Canada. The adequacy decisions for japan only cover private sector organisations. The adequacy finding for Canada only covers data that is subject to Canada's Personal Information Protection and Electronic Data Act. If you wish to transfer personal data to Japan or Canada you should seek specific legal advice as to whether you can rely on the partial adequacy decision.

B. Do I need to take any action?

☐ NO: I am receiving personal data from third countries but none of them are subject to an adequacy decision so I do not need to take any further action **(proceed to question 5)**

☐ YES: I am receiving personal data from a third country which is subject to an EU adequacy decision **(you need to take the action described in the below ACTION box. Make a note of this before you proceed to question 5)**.

ACTION: **In order to maintain its adequacy decision, the country or territory that is sending you personal data is likely to have its own legal restrictions on making transfers of personal data to countries outside of the EEA. UK officials are working with these countries and territories in order to make specific arrangements for transfers to the UK where possible. Where specific arrangements are not in place, you and the sender of the data will need to consider how to comply with local law requirements on transfers of personal data and seek local legal advice. You can find detail of the specific arrangements in place for each country that is subject to an adequacy decision on the ICO website at www.ico.org.uk (see the international data transfers page).**

5. Do I need to appoint an EU Representative?

A. Is this relevant to me?

☐ NO:

- ☐ I am not offering goods or services to individuals in the EEA or monitoring the behaviours of individuals in the EEA **(proceed to question 6)**; or
- ☐ I have one or more offices, branches or other establishments in the EEA **(proceed to question 6)**

☐ YES: I do not have any branches, offices or establishments in the EEA AND I am offering goods or services to individuals in the EEA or monitoring the behaviour of individuals in the EEA **(complete part B)**

B. Do I need to take any action?

☐ NO: **(if you only tick boxes in this section proceed straight to question 6)**

- ☐ I am a public authority

AND/OR

- ☐ my processing is only occasional, of low risk to the data protection rights of individuals, and does not involve using special category or criminal offence data on a large scale

☐ YES: I am not a public authority and… **(if you tick any boxes in this section you will need to take the action described in the ACTION box below. Make a note of this before you proceed to question 6)**.

- ☐ my processing is regular or routine; or
- ☐ my processing carries a risk to the data protection rights of individuals; or
- ☐ my processing involves using special category or criminal offence data on a large scale

ACTION: **You must enter into a written agreement with a representative based in one of the EEA states where some of the individuals whose personal data you are processing are located. Your representative may be an individual or a company or organisation established in the EEA and must be able to represent you in respect of your obligations under the EU GDPR (e.g. a law firm, consultancy or private company). Your agreement must authorise the representative to act on your behalf regarding your EU GDPR compliance and to deal with any supervisory authorities or data subjects in this respect.**

6. Do I need to identify a new lead Supervisory Authority?

A. Is this relevant to me?

☐ NO: I have one or no offices, branches or other establishments in EEA states (excluding the UK) AND my processing does not substantially affect individuals in any other EEA states **(proceed to question 7)**

☐ YES:

- ☐ I have offices, branches or other establishments in 2 or more EEA states excluding the UK **(complete part B)**; or
- ☐ I have offices, branches or other establishments in 1 or no EEA states excluding the EEA but my processing substantially affects individuals in 2 or more EEA states excluding the UK **(complete part B)**

Remember!

Once the UK exits the EU the ICO will no longer have standing to act as your lead Supervisory Authority.

B. Do I need to take any action?

☐ NO: I have already nominated a lead Supervisory Authority and it is not the ICO **(proceed to question 7)**

☐ YES: **(you need to take the action described in the below ACTION box. Make a note of this before you proceed to question 7)**

- ☐ my current nominated lead supervisory authority is the ICO; or
- ☐ I have not yet nominated a lead supervisory authority

> ***ACTION:*** **You should review the European Data Protection Board's (EDPB) guidelines to work out which Supervisory Authority you should nominate as your lead Supervisory Authority. Note that your lead Supervisory Authority must be located in the place of your main establishment in the EEA. This means your main administrative centre or the place where real exercise of management activities or decision making takes place. If you do not have a main establishment in the EEA it may not be possible to designate a lead Supervisory Authority. You can find a link to the EDPB guidelines on the ICO's website (via the EU regulatory oversight page).**

7. What steps might I need to take to update my records etc.?

A. Is this relevant to me?

☐ YES: this is relevant to all organisations **(complete part B)**

B. Do I need to take action?

☐ YES: all organisations should review what updates may be required and ensure that these are made **(you need to take the action described in the below ACTION box. Make a note of this before you finish the checklist)**.

> ***ACTION:*** **Review your privacy notices, Article 30 processing records, internal policy and procedure documents and any data protection impact assessments to ensure that (a) any changes to international transfers are reflected, (b) any references to 'Union law' or other terminology changed in the UK GDPR is updated and (c) your EU representative is identified (if you are required to have one).**

TIP! Keep a copy of your completed checklist to demonstrate that you have assessed what actions you may need to take to update your compliance measures for Brexit. Even if you decide that you do not need to make any changes, being able to demonstrate that you have given the issue proper consideration will help you meet the accountability requirements under the GDPR.

Do you need further advice? Please contact Kitty Rosser or call directly on 01603 756 559 for advice on all aspects of data protection compliance.

Please note that this briefing is not intended to set out legal advice but to provide a general overview of the issues and actions that may be relevant. It may help you identify whether you need to seek further advice but should not be seen as an alternative to taking specific legal advice.