Birketts
Clear Legal Advice

Brexit and GDPR: what you need to know and do

Kitty Rosser
Legal Director
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 compliance, there is no one size fits all solution. We have produced this briefing note and checklist to assist organisations in understanding and identifying the steps relevant to them.

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.

Who to contact for further advice

If you require specific legal advice on any of the issues covered in this briefing note please contact **Kitty Rosser** by email at kitty-rosser@birketts.co.uk or by telephone on 01603 756559.

Stay updated

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

Birketts
Clear Legal Advice

Headline issues to be aware of

What is the 'UK GDPR'?

The GDPR is an EU regulation that came into effect in May 2018 and was directly applicable in the UK until 31 December 2020 when the UK left the EU. Although the GDPR ceased to be directly applicable in the UK, the UK Government decided that it should continue to apply in the UK as retained EU law. The retained EU version of the GDPR is commonly referred to as the UK GDPR. It sits alongside the Data Protection Act 2018.

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**"). However, the EU Commission has recognised that the data protection laws in some third countries offer an equivalent level of protection to EU data protection laws. Such countries have been granted adequacy decisions. Personal data can continue to flow freely between third countries with adequacy decisions in place and EEA countries. Post-Brexit, the UK will also recognise existing adequacy decisions issued by the EU Commission so that data may continue to flow freely between the UK and those third countries that hold them. Following Brexit, the UK itself is also now a third country. If no adequacy decision is issued for the UK, future transfers of personal data from the EEA into the UK will only be allowed if certain safeguards are implemented, such as Standard Contractual Clauses. To keep personal data flowing in the immediate post-Brexit period the UK-EU Trade and Cooperation Agreement ('**TCA**') included a grace period of 4 months (extendable up to 6 months) from 1 January 2021. It is anticipated that the EU Commission will formally announce whether the UK will be granted an adequacy decision or not before the end of this grace period.

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

No. On the 16 July 2020 the Court of Justice of the EU handed down a landmark decision ("**Schrems II**") which stated that the EU-US Privacy Shield could no longer be relied on for transfers of personal data to the US. Transfers of personal data from the UK to the US may only take place if an appropriate safeguard, such as Standard Contractual Clauses, is in place or if a derogation applies.

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 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 currently 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. However, in November 2020, the EU Commission published a draft set of SCCs that cater for such transfers. The draft SCCs are currently under consultation and review and are expected to come into force

early 2021. In the meantime, the existing controller – processor and controller – controller SCCs can be used, including for transfers of data from the UK to third countries. 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. The ICO has produced a useful tool to enable organisations to quickly and easily prepare the appropriate SCCs. Importantly, following Schrems II, parties wishing to implement SCCs must first carry out an equivalence assessment. The purpose of this assessment is to identify whether any local laws in the data recipient's country may undermine the protections afforded by the SCCs. If the equivalence assessment determines that local laws do impinge on the effectiveness of the SCCs then supplementary measures must be implemented to ensure individuals remain properly protected. Where this is not possible the data transfer cannot proceed. The European Data Protection Board has published detailed guidance on what may constitute appropriate supplementary measures in these circumstances.

What are Binding Corporate Rules (BCRs)?

BCRs are intra-group data protection policies put in place to enable personal data to be transferred from group entities established in the EEA to group entities outside of the EEA. The policies must be legally binding and enforced by every relevant entity within the group. BCRs must be submitted to, and approved by, relevant Supervisory Authorities. Once they have been approved, they are considered an appropriate safeguard to enable personal data to be transfers outside of the EEA but they only apply to transfers taking place between members of the same group. Following Brexit, UK BCRs approved by the Information Commissioner are required for transfers of data from UK group entities to non-EEA group entities. Groups which are transferring data from both UK and EEA group entities to group entities outside of the EEA will need to have both EU BCRs and UK BCRs in place.

Who 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 was the Information Commissioner's Office ("**ICO**"). Post-Brexit, the ICO continues to be the UK data protection regulator but it has ceased to have standing as a Supervisory Authority under the GDPR.

What is the One Stop Shop?

This is a concept established by the GDPR to prevent organisations having to deal with multiple different Supervisory Authorities. Where an organisation has establishments in multiple EEA countries or an establishment in one EEA country only but undertakes processing activities that are likely to substantially affect individuals in other EEA countries it is said to be engaged in cross-border processing. Under the GDPR's one stop shop provisions an organisation engaged in cross border 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. Post-Brexit, UK organisations will still deal with the UK ICO in respect of their UK activities but will also deal with one or more Supervisory Authorities in respect of any activities in the EEA. In the event of breach they may face enforcement action and fines from multiple Supervisory Authorities as well as from the ICO.

What is an EU or UK Representative?

The GDPR has extra-territorial effect and applies to entities that are selling goods and services to individuals in the EU or monitoring the behaviour of individuals in the EU even the entity has no establishment in the EU. To ensure that individuals in the EU are properly protected in such cases, those non-EU entities are required to appoint representatives in the EU. The representative acts as a point of contact for interested Supervisory Authorities and individuals and can even be subject to data protection investigations and enforcements in the place of the non-EU entity. There are equivalent extra-territoriality provisions in the UK GDPR and so any entity that is selling gods or services to individuals in the UK or monitoring their behaviour but has no establishment here must appoint a UK representative.

Birketts
Clear Legal Advice

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 data protection compliance regime remains appropriate and compliant post-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 countries are still permitted after Brexit. No further action is required.

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. If you have BCRs in place please also see question 5.

B. Do I need to take any action?

☐ NO –

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

- ☐ Andorra
- ☐ Argentina
- ☐ Canada
- ☐ Faroe Islands
- ☐ Guernsey
- ☐ Israel
- ☐ Isle of Man
- ☐ Japan
- ☐ Jersey
- ☐ New Zealand
- ☐ Switzerland
- ☐ Uruguay

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 in place and I have conducted an equivalence assessment as required by Schrems II and put in place supplementary measures where needed

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 –

☐ 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 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.

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

A. Is this relevant to me?

☐ NO – I do not receive personal data from any EEA countries **(proceed to question 4)**

☐ YES – I do receive personal data from EEA countries **(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 in place together with supplementary protection measures where required under Schrems II

☐ MAYBE – I have not yet put SCCs and any appropriate supplementary measures in place. If the UK does not receive an adequacy decisions from the EU Commission I will need to address this

ACTION: **In the short term, continue to monitor the situation to see whether the UK receives an adequacy decision from the EU Commission. If it does not, then use the ICO's interactive tool "Keep data flowing from the EEA to the UK" to implement the appropriate SCCs or identify an alternative appropriate safeguard. The tool is available on the ICO's website at ico.org.uk. Remember that you will also need to undertake an evaluation assessment as required under Schrems II and implement appropriate supplementary protection measures where appropriate.**

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

A. Is this relevant to me?

☐ NO – I do not receive personal data from any 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. If you have BCRs in place please also see question 5.

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

☐ YES – I am receiving personal data from a third country which is subject to an EU adequacy decision

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 ico.org.uk (see the international data transfers page).**

5. Can I continue to reply on BCRs for intra-group transfers?

A. Is this relevant to me?

☐ NO - I do not use BCRs **(proceed to question 6)**

☐ YES – I do use BCRs **(complete part B)**

B. Do I need to take any action?

☐ YES – I need to ensure that I have UK BCRs in place for intra-group transfers from UK group entities to group entities outside of the EEA (I can no longer rely on my EU BCRs for this)

ACTION: **The specific process that you need to follow to obtain UK BCRs will depend upon whether your existing EU BCRs were authorised by the ICO and whether they were approved before or after 25 May 2018. Please refer to the ICO's guidance note, Binding Corporate Rules at the end of the transition period, which is available on the ICO website at ico.org.uk for details of the action required for your BCRs.**

6. 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 7)**; or
- ☐ I have one or more offices, branches or other establishments in the EEA **(proceed to question 7)**

☐ 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 –

- ☐ 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…

- ☐ 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 countries 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.**

7. Do I need to appoint a UK Representative?

A. Is this relevant to me?

☐ NO –

- ☐ I am not offering goods or services to individuals in the UK or monitoring the behaviours of individuals in the UK **(proceed to question 8)**; or
- ☐ I have one or more offices, branches or other establishments in the UK **(proceed to question 8)**

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

B. Do I need to take any action?

☐ NO –

- ☐ 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…

- ☐ 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 the UK. Your representative may be an individual or a company or organisation established in the UK and must be able to represent you in respect of your obligations under the UK GDPR (e.g. a law firm, consultancy or private company). Your agreement must authorise the representative to act on your behalf regarding your UK GDPR compliance and to deal with the Information Commissioner's Office or data subjects in this respect.**

8. 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 countries **AND** my processing does not substantially affect individuals in any other EEA countries **(proceed to question 9)**

☐ YES –

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

Remember!

The ICO no longer has 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

☐ YES –

- ☐ 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).**

9. 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

B. Do I need to take any action?

☐ YES – all organisations should review what updates may be required and ensure that these are made.

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 legislation or other terminology are appropriately updated and (c) your EU/UK 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. 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.