UK/EU data transfers after exiting the EU

Last updated January 2021

There's understandably been a lot of interest from members in the impact of Brexit on data flows to and from the EU. This guide explains some of the key concepts and signposts to some useful resources, although please be aware that it doesn't replace legal advice.[1]

What does the 'deal' mean for data flows?

Even though a wider EU exit 'deal' – the 'Trade and Cooperation Agreement' (the Agreement) – has been agreed between the UK and the EU (subject to ratification by the European Parliament), the EU is currently still assessing the UK's data adequacy' which follows a separate process, and has not yet reached a decision on that. However, as the UK has now left the EU, special provisions have been made in the Agreement for data transfers from the EU/EEA to the UK to be able to continue for the time being (though not indefinitely). This avoids a 'cliff edge' for data transfers while the adequacy process is concluded. The details are set out in Part 7 of the Agreement and summarised in this document.

What are the rules for data transfers from 1 Jan 2021?

The Agreement contains provisions to allow EU/EEA-UK data flows to continue on pre-existing terms for a maximum of six months. This 'bridging mechanism' allows data to be transferred in the same way it was pre-1 January 2021 (effectively, as if the UK were still a member of the EU) for a "specified period" of four months, extendable by a further two months, provided that the UK makes no changes to its rules on data protection in the interim.

The period will end when the European Commission (EC) adopts an adequacy decision in relation to the UK. If this has not happened by 1 April then the period will be extended by two more months to 1 June (unless either the UK or the EU objects).

The UK has already deemed the EU/EEA to be adequate on a transitional basis, meaning that data can also continue to flow freely from the UK to the EEA while the UK makes its own formal adequacy assessments.

Why are data transfers affected by Brexit?

Article 45 of the EU GDPR states:

[1] This guide does not cover other data transfer scenarios, e.g. UK to U.S.

‘A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.’

This basically means that for personal data to be transferred from the EU/EEA to a ‘third country’ (i.e. one outside of the EU/EEA, such as the UK), the European Commission needs to assess whether that particular country offers a level of personal data protection equivalent to that provided by EU law. 13 countries have been recognised by the European Commission as being adequate or partially adequate. The UK allows personal data transfers from the UK to the EU/EEA and to countries that have an existing EU adequacy decision (and will make its own adequacy decisions in due course, now it has left the EU). However, the European Commission still needs to make an adequacy decision about the UK’s personal data protection framework.

There is no guarantee that adequacy will be granted, but the way in which the Agreement explicitly references adequacy, and the fact that the UK has implemented GDPR (see below for more details) gives some grounds for cautious optimism.

Does the GDPR still apply to the UK?

The GDPR is EU law and as such, no longer applies directly to the UK – although it may still apply to individual companies in the UK, depending on your activities (see below). However, GDPR was implemented in the UK in 2018 and as part of the Brexit arrangements, the UK ‘retained’ it as UK law after we left the EU. It will continue to apply together with the Data Protection Act 2018. It has been renamed UK GDPR, but it is largely the same as the EU GDPR.[2]

Both the EU GDPR and the UK GDPR have ‘extra-territorial’ scope which means they can apply to companies outside of the EU or the UK, respectively, and you may need to comply with relevant requirements (such as the need to appoint a representative). The ICO’s website has advice on data protection post-Brexit, and you should seek appropriate legal advice as necessary to ensure you understand your obligations.

What do I need to do now?

You can receive data from the EU/EEA without needing to put in place any additional provisions until at least 1 April 2021. However, if your business depends on this data, then it would be sensible to look at putting in place contingency arrangements, such as Standard Contractual Clauses (SCCs) (see below), to avoid future disruption. The Information Commissioner’s Office (ICO) recommends doing this, and more

[2] Some technical changes have been made to reflect the UK’s changed status, such as provisions relating to cross-EU regulatory cooperation. You should seek appropriate legal advice as necessary.

guidance is available for businesses in their Brexit advice hub. The Government has also published guidance on how Brexit affects data protection.

You should also review your documentation such as contracts, terms and conditions, and privacy policies and notices, to reflect the changes to the UK's status as an EU member state and applicable law.

What are SCCs?

Broadly, SCCs are a standard set of contractual terms and conditions for the transfer of personal data which both the data exporter and the data importer enter into. They include contractual obligations that help to protect personal data when it leaves the EU/EEA, and to ensure compliance with the EU GDPR. SCCs only relate to the transfer of personal data, so they can be incorporated into a wider contract that covers other business terms. One of the key benefits of SCCs is that they come with the European Commission's seal of approval.

How can SCCs help?

Article 46 of the EU GDPR says that in the absence of an adequacy decision, personal data may be transferred to a third country or an international organisation only if the controller or processor has provided appropriate safeguards. Such safeguards would therefore be necessary if adequacy has not been granted to the UK by the end of the period specified in the Agreement.

There are a number of recognised safeguards, one of which is SCCs, and these are likely to be the most appropriate ones for many businesses for transfers of personal data from the EU/EEA to the UK (for multinationals based in the UK and operating in one or more EU/EEA States, Binding Corporate Rules are appropriate for inter-Group cross border personal data transfers).

The European Commission issues SCCs that cover the transfer of personal data. These are in the process of being updated. They currently cover transfers of personal data:

- from data controllers in the EU to data controllers established outside the EU/EEA (controller to controller).
- from data controllers in the EU to processors established outside the EU/EEA (controller to processor).

If you need to transfer personal data from an EU/EEA-based processor to your UK-based organisation, there are currently no European Commission-approved SCCs for this scenario. If the processor has a controller also located in the EU/EEA you may be able to use the 'controller-to-controller' SCCs. In any case, the EU/EEA based processor will be subject to certain GDPR provisions that are applicable to data processors. You may need to seek legal advice on an appropriate mechanism to enable the flow of data.

The new draft SCCs cover transfers from:

- controller to controller
- controller to processor
- processor to controller
- processor to processor

The new SCCs are yet to be approved and adopted by the European Commission. Once this happens, organisations will have 12 months to replace their existing SCCs. Until then, current SCCs will apply.

How do I use SCCs?

The Information Commissioner's Office (ICO) has developed a tool for small and medium-sized businesses and organisations to help them decide if SCCs are appropriate and to select the right one. You can use the SCCS as standalone contracts or incorporate them into a wider contract but you cannot amend the SCCs themselves, or they will no longer be authorised by the European Commission or relevant Data Protection Authority.

You should also be aware that the guidance on the use of SCCs changed in 2020, particularly in relation to carrying out risk assessments when using SCCs. For more details see our update on the privacy shield and the Government's guidance.