

Data Protection and Brexit – Frequently Asked Questions



Countries in the EU have very high standards of data protection, particularly under the provisions of the General Data Protection Regulation (GDPR). EU-based data controllers (those who decide how and why personal data are processed) are not permitted to transfer personal data outside the EU/EEA unless those standards are maintained.

Brexit will have a serious impact on the data protection obligations of Irish controllers which transfer personal data to the UK (including Northern Ireland); because, in a situation where the UK becomes a 'third country', transfers to the UK will be considered transfers outside of the EU/EEA and will require a mechanism to ensure an adequate level of data protection.

In what situations might Brexit impact an organisation?

There are many ways in which Irish-based organisations may be involved in transferring personal data to the UK, including as part of e-commerce transactions, arrangements with partner organisations, and support services such as software provision or cloud hosting. The following is a non-exhaustive list of questions we encourage organisations to consider in order to assess the impact of Brexit on their processing arrangements:

- ☐ Are you outsourcing your HR, IT, or payroll function to a UK-based organisation?
- ☐ Are you storing data in the UK on a server or in the cloud?
- ☐ Are you using software (such as email, CMS, or databases) provided by a UK-based company which may involve transfer of personal data to a UK server?
- ☐ Are you using a UK-based marketing company to send marketing communications to your customer database?
- ☐ Are you using a UK-based company to analyse data on visitors to your website?
- ☐ Are you using translation/transcribing services of a UK-based company where you might be sending personal data of employees, customers, or suppliers?
- ☐ Is your occupational health provider based in the UK?
- ☐ Is your pension scheme based in the UK?

What happens if there's a negotiated deal?

If there is a negotiated deal to regulate the UK's relationship after it leaves the EU and/or during any transition period, then the exact effects on data transfers, will depend on the nature of that deal, particularly if there's an adequacy decision. As the matter progresses, we will update our guidance accordingly.

What happens if there's a 'No Deal' Brexit?

In a 'No Deal' Brexit scenario, the UK will leave the EU/EEA with no arrangements to ensure adequate levels of data protection in place, therefore it will be treated as any other 'third country' without an adequacy decision.

In these circumstances, an Irish-based controller intending to transfer personal data to the UK will need to utilise a mechanism providing specific safeguards to ensure an adequate level of protection for that data. This can be done in a number of different ways, depending on the circumstances in which the data is to be transferred, which is outlined in further detail below.

What mechanisms allow personal data to be transferred to the UK if it becomes a 'third country'?

The GDPR sets out a number of mechanisms intended to ensure adequate protection of personal data which are transferred outside of the EU/EEA to 'third countries'. The most relevant mechanisms in the context of Brexit are set out briefly below.

Adequacy Decision

Certain 'third countries', such as Japan, Israel, or New Zealand, have received what is known as an 'adequacy decision' from the European Commission. This allows a cross-border personal data transfer from the EU to that country, because it has been determined to have an adequate level of data protection safeguards compared to the EU. This is a very useful mechanism for controllers, as it allows transfers to the 'third country' almost as though it were a member of the EU and subject to the GDPR.

There is currently no adequacy decision in place regarding the UK, but one could be agreed post-Brexit, if the EU Commission finds the level of protection to be sufficient. In the interim one of the other mechanisms must be used.

Standard Contractual Clauses (SCCs)

One common mechanism for ensuring the protection of personal data transferred outside of the EU is the use of 'standard contractual clauses' (SCCs). This is likely to be relevant to most Irish-based controllers that transfer personal data to the UK. Further

details on SCCs can be found in our related guidance on [‘Transfers of Personal Data from Ireland to the UK in the Event of a ‘No-Deal’ Brexit’](#).

The SCCs consist of standard or template sets of contractual terms and conditions that the Irish-based controller and the UK-based recipient (often acting as a data processor) both sign up to. The basic idea is that each of the parties to the contract gives contractually binding commitments to protect personal data in the context of the transfer. Importantly, the data subject is also given certain specific rights under the SCCs even though they are not party to the relevant contract. Controllers and processors are encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.

The SCCs can be adopted by putting in place a standalone or new contract between the Irish-based controller and the UK-based recipient. As well as setting out the SCCs, that contract may also include other commercial clauses provided those other clauses do not affect the operation of the SCCs or reduce data subjects’ rights. Where the Irish-based controller and UK-based processor already have a contract in place between them, as required by Article 28(3) GDPR, they may decide to incorporate the SCCs into that existing contract. Again, this is provided that its terms do not affect the SCCs or reduce the data subject’s rights.

To date, the European Commission has issued three sets of SCCs, which controllers may want to consider as a mechanism for transferring personal data to the UK post-Brexit. Two sets are intended for data transfers from EU controllers to non-EU controllers (Set I [Decision 2001/497/EC](#) and Set II [Decision 2004/915/EC](#)), and one set is for data transfers from EU controllers to non-EU processors (Set III [Decision 2010/87/EU](#)). (See paragraph below for information relating to updated SCC’s.

Binding Corporate Rules (BCRs)

One mechanism which might be relied upon by multinational groups of undertakings or a group of enterprises engaged in a joint economic activity are ‘binding corporate rules’ (BCRs). BCRs involve a legally binding internal code of conduct operating within a multinational group, which applies to transfers of personal data from the group’s EEA entities to the group’s non-EEA entities.

There are two types of BCRs which can be approved: BCRs for controllers which are used by the group entity to transfer data that they have responsibility for, such as employee or supplier data; and BCRs for processors which are used by entities acting as processors for other controllers and are normally added as an addendum to the Service Level Agreement or data processor contract. BCRs must include all essential principles and rights to ensure appropriate safeguards for transfers of personal data.

BCRs are legally binding data protection rules with enforceable data subject rights contained in them, which are approved by the competent supervisory authority, such as the Data Protection Commission (DPC). For new BCRs, controllers will not be able to rely on them to transfer personal data to an entity in the UK until they have been formally approved by the supervisory authority and the European Data Protection Board (EDPB). But if an Irish entity is already a member of a group with an approved BCR they can continue to transfer data to the UK entities also covered by the BCR.

The European Commission are working on new SCC's, should controllers wait until they are adopted?

The current SCC's listed above are still a valid mechanism for use until they are repealed or replaced. So Irish based controllers should not delay or defer signing SCC's with the UK data importer. There must be a valid mechanism in place before the end of the transition period. However once the new SCC's are finalised, they will need to be updated and signed.

Does the Judgment in the 'Schrems case' have any impact?

Yes. In it's judgment the court examined the validity of the 2010 SCC's decision and considered that it is still valid. However the Court added that the SCC's only remain valid if they provide a level of protection essentially equivalent to that guaranteed within the EU by the GDPR. The SCC's themselves place obligations on the data exporter to verify whether that level of protection is respected in any third country, prior to making the transfer.

The SCC's also require the data importer to notify the exporter of any issues they might have with complying with the clauses and to allow the data exporter to determine if it is possible to put in place supplementary measures to overcome the issues. If this is not possible the Irish based data controller must suspend or end the transfer.

Where can I find further guidance materials regarding Brexit?

We encourage controllers to consult our previous guidance on Brexit and international transfers of personal data, namely ['Transfers of Personal Data from Ireland to the UK in the Event of a 'No-Deal' Brexit'](#) and ['Transfers of Personal Data to Third Countries or International Organisations'](#).

Controllers should consult the [website of the UK Information Commissioner's Office \(ICO\)](#) for guidance on how to comply with UK rules on data protection post-Brexit, in particular their guidance on ['Data Protection and Brexit'](#). The Government of Ireland has

also made a number of resources available, on various aspects of Brexit, on their [‘Getting Ireland Brexit Ready’](#) webpage.

Controllers should also consult the EDPB website for information on the [Judgment](#) and also [Supplementary measures](#).