Data Protection and Brexit – Frequently Asked Questions

An Coimisiún um Chosaint Sonraí
Data Protection Commission

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, particularly in the context of a 'No Deal' scenario, may 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 during the 'transition period'?

The UK formally left the European Union on 31 January 2020, but entered a Brexit 'transition period'. During this period, which is currently expected to run until the end of December 2020, the GDPR still applies in the UK, so arrangements for transferring personal data to or from the UK remain unchanged. Controllers will be able to continue to transfer personal data to the UK as before, until such a point as the transition period ends and/or a new agreement regarding data protection is reached.

Even though there is a transition period, we encourage controllers to plan their data transfer arrangements in the event that further negotiations result in some form of negotiated deal or a 'No Deal' Brexit that changes the nature of data protection in the UK and its relationship with EU data protection law.

What happens if there's a negotiated deal?

If there is a negotiated deal to regulate the UK's relationship at the end of the transition period, then the exact effects on data transfers will depend on the nature of that deal. As the matter progresses, we'll do our best to update our guidance accordingly.

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

In a 'No Deal' Brexit scenario, the transition period will end with no arrangements to ensure adequate levels of data protection in place, therefore the UK 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 will be discussed 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 it is possible that an adequacy decision could be made in the future, where the EU Commission finds the level of protection to be sufficient. However, this process would not be automatic, and, if compared to the previous adequacy decisions, could take a number of months or years to finalise.

It is possible that the transition period (in which the UK remains subject to the GDPR) could allow time for the EU Commission to work on an adequacy decision. Nevertheless, this mechanism is unlikely to be available to controllers in the short term.

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 previous 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).

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). Where BCRs were approved prior to the GDPR, but have been updated in light of the GDPR and notified to the supervisory authority, no new formal approval is required.

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.