Brexit — impact on personal data flows between Ireland and the UK

Ian Duffy, Associate with Arthur Cox, advises Irish organisations making personal data transfers to and from the UK on how to prepare for the various outcomes after the UK leaves the EU

The UK is due to leave the EU on 29th March 2019. Despite this looming deadline, uncertainty remains as to how Brexit will affect personal data flows between Ireland and the UK. With little time remaining, many organisations across Ireland and the UK can no longer wait for the political fog in Westminster to clear, and are looking at the steps they can take to continue to lawfully transfer personal data between Ireland and the UK after the withdrawal date, regardless of the impending outcome on Brexit.

With this in mind, this article outlines how personal data flows between Ireland and the UK will be affected in the event of:

- a Brexit deal that aligns with the position on data and transition from the UK government's withdrawal agreement (25th November 2018) and the political declaration for the future relationship agreed on 22nd November 2018 between the UK government and the EU (i.e. a negotiated agreement); and
- a 'no deal' Brexit.

It will also look at the steps that organisations may wish to take now in order to safeguard personal data transfers between Ireland and the UK, regardless of whether there is a negotiated agreement or no deal.

Impact of negotiated agreement

If the UK leaves the EU on the basis of a negotiated agreement, there will be no immediate disruption to personal data flows between Ireland and the UK following the withdrawal date. Instead, there will be a transition period up to 31st December 2020 during which the UK will continue to be subject to EU law (including EU data protection laws), and personal data will be able to flow between Ireland and the UK without the need for additional safeguards, such as EU-approved Standard Contractual Clauses).

Put another way: if an organisation lawfully transfers personal data between Ireland and the UK prior to the withdrawal date, a negotiated agreement will mean that this organisation does not need to take any additional steps to continue lawfully transferring personal data between Ireland and the UK after the withdrawal date (at least for the transition period).

It is the intention of the UK and the EU that the free flow of personal data from the European Economic Area ('EEA' which is comprised of EU Member States, Iceland, Liechtenstein and Norway) to the UK will also continue after the transition period. Under a negotiated agreement, the European Commission will assess the UK's post-Brexit data protection laws with a view to reaching a decision that these laws provide an adequate level of data protection. If the European Commission reaches this decision, additional safeguards will not be required to lawfully transfer personal data from the EEA (including Ireland) to the UK. Instead, the UK will benefit from what is referred to as an adequacy decision.

Jurisdictions that currently benefit from an adequacy decision include Argentina, Guernsey, Israel, the Isle of Man, Jersey, New Zealand and Switzerland. More details on the countries that currently benefit from adequacy decisions may be found at www.pdp.ie/docs/1084

Impact of no deal

The impact of no deal will vary depending on whether personal data are transferring from the UK to Ireland or vice versa.

For UK to Ireland data flows: The UK Department of Digital, Culture, Media & Sport issued guidance on 13th December 2018 confirming that the UK will transitionally recognise all EEA states, EU and EEA institutions and Gibraltar as providing an adequate level of protection for personal data. This means that personal data can continue to flow freely from the UK to any EEA country (including Ireland) and Gibraltar in a no deal scenario without the need for additional safeguards (such as EU-approved Standard Contractual Clauses).

The UK intends to keep this recognition under review in the event of a no deal, but it seems unlikely that this position will change, certainly in the short to medium term at least.

The key point is therefore that in a

no deal scenario, an organisation that already lawfully transfers personal data from the UK to Ireland will be able to continue lawfully doing this post-Brexit without taking any additional steps.

For Ireland to UK data flows: No deal will be more disruptive to transfers of personal data from Ireland to the UK. In such scenarios, the UK will become a 'third country' under the General Data Protection Regulation (the 'GDPR'), meaning that it does not provide an adequate level of data protection. As a result, Irish-based organisations will need to put in place additional safeguards to protect personal data that they transfer to the UK. Some safeguards that could be deployed by Irish-based organisations in order to continue lawfully transferring personal data to the UK in a no deal scenario are discussed below in the 'Protecting Ireland to UK data flows against no deal' section.

"No deal will be more disruptive to transfers of personal data from Ireland to the UK. As a result, Irish organisations will need to put in place additional safeguards to protect personal data that they transfer to the UK."

It is possible that in a no deal scenario, these safeguards may only need to be temporary in nature. The UK government has indicated that in the event of no deal, it intends to seek an adequacy decision from the European Commission so that personal data can continue to flow freely from the EEA to the UK. However, the European Commission has stated that an adequacy decision cannot be made in respect of the UK until it becomes a 'third country' (which will be 30th March 2019 at the earliest) and traditionally, the European Commission takes a significant period of time to reach an adequacy decision.

As a result, any adequacy decision that the European Commission may grant to the UK in a no deal scenario will not remove the need for additional safeguards to protect transfers of personal data from Ireland to the UK until such adequacy decision comes into effect.

Protecting Ireland to UK data flows against no deal

As a first step, organisations should review their data flows, and identify and document all instances where they transfer personal data from Ireland to the UK. If there is no reason why these data flows should be discontinued in a no deal scenario, the organisation should put in place one of the additional safeguards in the GDPR that facilitate the lawful transfer of personal data to a third country (such as the UK in a no deal scenario).

Set forth below are the more relevant safeguards for most organisations:

Standard Contractual Clauses: Standard Contractual Clauses are likely to present the most pragmatic and simplest safeguard for many organisations to continue lawfully transferring personal data from Ireland to the UK in a no deal scenario. In effect, this safeguard involves the Irish-based organisation and the receiving organisation in the UK entering into a contract based on Standard Contractual Clauses approved by the European Commission.

These clauses are designed to ensure that the receiving organisation in a third country is contractually bound by obligations that ensure personal data will benefit from an adequate level of data protection when transferred to that third country. There are a number of sets of Standard Contractual Clauses which are available at www.pdp.ie/docs/1085. The appropriate set of clauses will depend on whether the receiving organisation in the UK is acting as controller or processor.

Data subject consent: Another possibility is to obtain the consent of relevant data subjects to the transfer of their personal data from Ireland to the receiving organisation in the UK. For large datasets, this is likely to prove challenging. In addition, it is difficult to obtain a valid consent under the GDPR and even if you do, this consent may be withdrawn at any time. As a result, this safeguard may not be practicable for many organisations.

Performance of a contract: The GDPR will permit an organisation to transfer personal data from Ireland to the UK where such transfers are necessary for the performance of a contract between that organisation and the relevant data subject. This may be helpful for one-off transfers or small-volume transfers, but again, for large datasets, demonstrating that personal data are transferred for that purpose in every instance may be administratively burdensome and impracticable.

Other steps

In addition to putting in place an appropriate GDPR safeguard, there may be a number of other challenges facing organisations that wish to protect personal data transfers from Ireland to the UK in a no deal scenario. For example, some contracts may include prohibitions on transfers of personal data outside of the EEA, and in a no deal scenario, this will contractually prevent an organisation from transferring personal data from Ireland to the UK. Irish-based organisations should check all of their contracts for such a prohibition and where necessary, amend them to ensure that personal data may be transferred from Ireland to the UK in a no deal scenario.

The GDPR also requires organisation's privacy notices to include details of transfers of personal data to third countries. Again, in a no deal scenario, the UK will be a third

(Continued on page 6)

(Continued from page 5)

country for GDPR purposes and in such circumstances, Irish-based organisations should update their privacy notices to inform data subjects that transfers of their personal data to the UK post-Brexit will constitute transfers outside of the EEA.

Conclusion

Brexit presents challenges to personal data flows between Ireland and the UK which are only magnified by the continuing uncertainty as to Brexit's form.

However, organisations can take steps now to mitigate the risks Brexit presents to these personal data flows, regardless of whether there is a negotiated agreement or no deal. Doing so is particularly important for organisations that are transferring personal data from Ireland to the UK.

For many such organisations, putting in place appropriate EU-approved Standard Contractual Clauses, and reviewing their contracts and privacy notices, will go a long way towards mitigating the risk that Brexit presents to their personal data transfers to the UK.

Ian Duffy
Arthur Cox
ian.duffy@arthurcox.com