Brexit -Data Protection Overview

As it is unclear if and when an adequacy decision will be made in favour of the UK, Businesses will have to rely on alternative bases to transfer personal data from the EU to the UK.

The Data Protection Framework in the UK Post-Brexit

The EU General Data Protection Regulation (the "GDPR") is the principal piece of data protection legislation in the EU. On March 29, 2019 the provisions of the GDPR will be incorporated into UK law by the European Union (Withdrawal) Act 2018 (the "Withdrawal Act") and the GDPR will therefore remain the core law on data protection in the UK after that date (subject to amendments to make the mechanics of the legislation work in light of the UK's new status). Therefore, there will be no immediate change in respect of the data protection framework in the UK. In essence, post-Brexit there will be two versions of the GDPR – the existing EU version and a new UK version.

Transferring Personal Data Out of the EU Post-Brexit

The GDPR permits a free flow of personal data between EU member states. Transfers out of the EU are, however, only permitted in specific circumstances.

When the UK ceases to be an EU member state and therefore becomes a "third country" for the purposes of the GDPR, when transferring personal data from the EU to the UK, Businesses will need to ensure we have a valid basis for doing so.

Under the GDPR, subject to certain limited exceptions, personal data can only be transferred out of the EU where:

- the European Commission has determined that the country to which the personal data is being transferred "ensures an adequate level of protection" (an "adequacy decision");
- prescribed "appropriate safeguards" have been put in place, or
- the individual to whom the personal data relates has given their explicit consent to the transfer (having been informed of the possible risks).

Adequacy Decision

The UK government has made it clear that it is aiming for an "adequacy decision" to be made by the European Commission permitting transfers to the UK and that it is ready to begin adequacy assessments. The UK will have to show that it can provide an adequate level of protection in respect of personal data. The UK's level of protection would be adequate if personal data protection was essentially equivalent to the protection provided under the GDPR.

The UK's position will be unique, owing to the degree of regulatory alignment which has resulted from the UK's membership of the EU and incorporation of the GDPR into UK law. However, national crime and national security legislation can be a crucial factor. For example, the U.S. government's extensive investigatory powers are a key reason why there is no general adequacy decision in respect of the U.S. Similar concerns could potentially be raised with respect to the UK – the UK Investigatory Powers Act 2016 has been found, by the UK High Court, to violate the right to privacy under Article 8 of the European Convention on Human Rights. There is, therefore, some doubt whether a positive finding of adequacy will be made. The European Commission has, however, indicated that the "quickest and most efficient legal framework for the exchange of data with the UK" will be desirable "for the sake

of business interests." Overall, it seems likely that there will be an adequacy decision with respect to the UK. The question is, when?

The timing of any adequacy decision is uncertain. The UK government has indicated that it has approached the European Commission to start discussions regarding an adequacy assessment, but the European Commission has stated that the adequacy decision cannot be made until the UK becomes a third country. It has not given any guidance on a timeline for when these discussions may start. The GDPR requires certain factors to be assessed and certain procedural steps to be taken before an adequacy decision is made. This procedure could last many months after discussions are started.

In short, Businesses cannot simply assume that there will necessarily be an adequacy decision in place from March 29, 2019.

Alternative Bases for Transfers

If no adequacy decision is made, or at least not in time, there are a number of existing transfer mechanisms that may be put in place.

Standard Contractual Clauses

Standard contractual clauses (also known as model clauses) are contractual clauses that have been adopted by the European Commission. The clauses should be used in the precise form approved by the European Commission, although they can be supplemented by additional commercial terms. The clauses include contractual obligations between the data exporter and data importer and also include rights that are enforceable by data subjects. Many of our contracts already include model clauses but a full review is being undertaken.

The most appropriate and relevant mechanism for legitimising EU to UK personal data transfer (in the absence of an adequacy decision) is likely in many cases to be the implementation of standard contractual clauses. Provided it is clear what personal data is being exported, who the personal data will be transferred to, and how it will be processed, the clauses can be implemented relatively swiftly and without a formal application process.

Binding Corporate Rules

Binding corporate rules are rules to govern the transfer of data between entities within a multinational group of companies. The rules must be agreed with appropriate data protection authorities through an application process. It would be unlikely that businesses could get BCRs drafted and approved in time for the March deadline.

Consent

Personal data can be transferred out of the EU where the data subject has given their informed consent. Consent is, however, not a reliable mechanism for transfers, as consent can be withdrawn at any time. It is also unlikely to be appropriate in respect of any personal data of employees.

Transferring Personal Data Out of the UK Post-Brexit

The UK government has suggested that it intends for businesses within the UK to continue to be able to transfer data to the EU without any restrictions. It is anticipated that the UK will promptly adopt an adequacy decision in respect of the EU, or otherwise provide for the free flow of data to the EU – for

example, by providing that the EU does not constitute a "third country" for the purposes of the UK version of the GDPR.

Other Considerations

While international transfers of personal data are the most prominent data protection concern associated with Brexit, it is likely to have an impact on a number of other issues under the GDPR.

Lawful Basis

All processing of personal data must be covered by a "lawful basis." One lawful basis is that the processing is necessary for compliance with a legal obligation under EU or EU member state law. After Brexit, a legal obligation under UK law will not constitute a lawful basis for processing under the EU version of the GDPR. Similarly, an obligation under EU or EU member state law is unlikely to constitute a "lawful basis" under the UK version of the GDPR.

Businesses will need to rely on an alternative lawful basis. (May become more relevant when we talk about data pooling if the pool resides in the UK) The most appropriate basis will often be that the processing is necessary "for the purposes of legitimate interests." However, reliance on this basis requires businesses to conduct a balancing exercise to ensure that the data subjects' interests do not override the legitimate interests.

UK/EU GDPR Overlap

Given the extra-territorial effect of the GDPR, many businesses post-Brexit could be subject to both the EU and UK versions of the GDPR. While the requirements in the UK will remain substantially the same, UK government ministers will have powers to amend the UK version of the GDPR to better account for its separation from the EU. We should be aware that discrepancies may arise post-Brexit between UK and EU data protection obligations, which may both apply in respect of the same processing (for example, where a UK establishment processes personal data about individuals who are in the EU in relation to offering goods or services to such individuals).

Processors' Rights To Derogate From Controllers' Instructions

The GDPR permits data processors to deviate from the data controller's instructions only where required by EU or EU member state law. After Brexit a data processor processing personal data pursuant to the EU version of the GDPR that is subject to a UK legal obligation will not be exempt from complying with the data controller's instructions in order to comply with that legal obligation. They may therefore face a difficult choice of complying with UK law, or complying with their obligations under the EU version of the GDPR and to the data controller.

Conclusion

Last-minute back door compromises are a frequent aspect of EU negotiating but compromise this time is being left later than usual. Given the potential atmosphere, a prompt adequacy decision by the European Commission with respect to the UK should not be seen as a foregone conclusion.

Although the UK government has given positive indications that the status quo will be maintained for transfers out of the UK, there remains little certainty as to how this will be achieved.

Businesses should prepare for a disorderly Brexit. The Data Protection Commission has issued guidance on their website which is available at https://www.dataprotection.ie/en/news-media/latest-news/dpc-issues-important-message-personal-data-transfers-and-uk-event-no-deal .

Should you have any queries or concerns, please do not hesitate to contact the IDPAA on +353(0)872681891 or admin@idpaa.eu where our advisors will be able to guide you in your approach.

ISSUE	"NO DEAL"	"DEAL"	
	FROM 30 MARCH 2019	**TRANSITION PERIOD: 30 MARCH 2019 – 31 DEC 2020**	**POST-TRANSITION: 1 JAN 2021 –**
UK to EU transfers	No change	No change	No change
EU to UK transfers	Transfers restricted	No change	UK hoping to have achieved an adequacy decision; otherwise transfers restricted
Applicable laws	GDPR does not have direct effect. Potential for dual regulation: "UK GDPR" * + extraterritorial reach of "EU GDPR"	GDPR continues to have direct effect as UK law	GDPR does not have direct effect. Potential for dual regulation: "UK GDPR" * + extraterritorial reach of "EU GDPR"
Representatives	UK companies require EU representatives	No change	UK companies require EU representative