Introduction

Two options exist at present for Brexit: the negotiated Brexit, and a “no-deal” Brexit. Regardless of which of these options is selected by the UK Government, and assuming they stick to the timetable, on October 31st 2019 at 11 p.m. the UK will officially leave the European Union, as per the invocation in March 2017 of Article 50 of the Treaty on European Union (TEU).

This departure, however, doesn't mean that all European laws will immediately no longer apply. In particular, GDPR will continue without interruption as the law of the land, as it is largely brought into British law by the revised Data Protection Act (2018). The EU Withdrawal Act 2018 (EUWA) is the enabling legislation that retains the GDPR in UK law, and which allows the UK government to make changes to GDPR which are generally not available to EU member states.1

The Data Protection Act ensures that GDPR will continue in a slightly modified form known as Applied GDPR. The Act also confirms some aspects which are not part of GDPR, such as the existence of specific criminal acts, and associated fines and penalties. The EUWA also ensures that EEA countries (and Gibraltar) are recognised by the UK as jurisdictions with adequate data protection—however, this is unilateral and doesn't confer adequacy on the UK from the EU perspective.

The EUWA also will recognise EU Standard Contractual Clauses (SCC) in UK law and gives the ICO the power to issue new clauses. Binding Corporate Rules (BCR) will also be officially recognised under UK law under the EUWA—but note this is again unilateral, meaning some BCR will be invalid.

1 Typically, GDPR allows minor changes, such as lowering the age of digital consent from 16 to 13 years, as some member states have done. The UK, however, plans to make more significant changes, which potentially could lead to a considerable divergence between the UK “Applied GDPR” and “EU GDPR.”
PECR & ePR

Related to this is the Privacy for Electronic Communications Regulation (2003), also known as PECR, which is the current UK law concerning electronic marketing communications. PECR is based on a European directive from 2002, which is likely to be replaced during 2019 by the new ePrivacy Regulation (ePR). This new regulation was initially intended to go into effect at the same time as GDPR; however, it was delayed, and since it’s still in the drafting process, is unlikely to go into effect until 2021, well after Brexit.

Despite this, the British government has clearly stated that the ePR will be adopted into British law, at the same time that PECR is repealed—and like GDPR, most likely this will be an updated version of PECR, repealing and replacing the old PECR from 2003.

3rd Country Status

The third thing that will happen is the UK will immediately be regarded as a third country for data protection purposes, meaning that it will lose its automatic claim for adequacy. This means that any Controllers who are transferring data of EU residents to the UK for processing may not do so without an appropriate transfer mechanism. Instead, there should be a contract in place with the approved SCCs, or an approved Code of Conduct, or other valid mechanism. Note however that some mechanisms are valid only for limited period use, such as consent.

So why doesn’t the UK simply acquire an adequacy ruling as part of its Brexit agreement? Good question. The answer is that this might not be so simple. The European Commission recently gave the Japanese government an adequacy ruling as part of their complex trade deal, which took years to negotiate. The ICO has warned of their uncertainty of how long this will take. It might be part of a negotiated Brexit – but that is not guaranteed.

In the case of a no-deal Brexit, adequacy is not a given. One consideration is that there is some suggestion that the UK’s Data Protection Act, and in particular Parts III & IV (relating to Police and Security Services), not to mention exemptions for control of immigration, have the potential to be seen as blockers for an easy negotiation towards a UK adequacy arrangement with the European Commission. Therefore, prudent businesses will already be switching to a contract based on approved SCCs, where they need to transfer personal data from the EU/EEA to the UK.

The Day After and the EDPB

So, let’s think about what happens the day after Brexit. Firstly, the ICO will no longer be a voting member of the European Data Protection Board (EDPB) and therefore will no longer have any influence on GDPR policies and interpretations. It may have observer status, like Norway or Iceland, but this may depend on whether the UK joins the European Economic Area – a position which has been rejected by the government. Therefore, this status is not guaranteed.

BCR Woes

The second thing which happens is that the ICO loses its status as the anchor for a dozen or so Binding Corporate Rules (BCR), for which Britain is the leading authority. The impact of this is limited to those dozen mostly British companies which signed up to the BCR several years prior to GDPR. They know who they are, and their legal counsels are already prepared with a replacement, probably based on Standard Contractual Clauses (SCC). So, there’s no need for most UK businesses to worry about that.
EU Representation and Article 27

The fourth implication of withdrawal is that companies based in the UK will, under Article 27, and if they meet the risk threshold, require the appointment of an EU Representative in one or more EU states, depending on where most of their customers reside. This is complicated by the fact that Article 27 remains part of the UK’s own “applied GDPR”, suggesting there may need to be a reciprocal arrangement for EU companies requiring the as-yet unspecific “UK Representation.” Either way, it’s a huge potential mess, made even worse in the event of a no-deal Brexit. The EUWA obliges non-UK controllers who are subject to the UK data protection framework to appoint representatives in the UK if they are processing UK data on a large scale.

So, What If There’s No Deal?

According to the ICO, if there is a Brexit deal, this will enable a transition arrangement that grants temporary adequacy until 31 December 2020, until “a longer-term solution can be put in place”, i.e. a proper adequacy arrangement. However, if there is no deal, then data flows of personal information from the EU can potentially be endangered without additional measures.

Conversely, in the event of no deal, the UK government has said there will be no legal restrictions on the transfer of data from the UK to EEA countries (i.e. the UK plus Norway, Iceland, Switzerland, etc). However, this doesn’t solve all problems for British companies.

In the case of EU visitors whose data is being collected by UK businesses, there’s no problem because consent is being given at the individual level. This approach however doesn’t work for B2B transfers of personal data. Furthermore, such consent is only valid for exceptional transfers, and is not suited for long-term regular transfers of personal data.

In practical terms, it’s going to be a problem if companies are more concerned about compliance than business matters. Operating without a lawful basis for transfer, in theory, may not result in prosecution, unless there is a complaint. This is because European data protection authorities are unlikely to make such prosecutions a priority. However, how long this will last is an interesting question; this is likely to depend on the risk appetite of the businesses and their European partners.

The bottom line – adhere to GDPR because it’s the right thing to do and because the risks of non-compliance could lead to future problems, and potential legal issues, which could go to court. Reputational risk is also real.

ECHR & CJEU

It’s important (and we think interesting) to note that GDPR is ultimately an expression of human rights law. The European Court of Human Rights (ECHR) is an international court that was established by the European Convention on Human Rights, which precedes the European Union, having been established in 1959. The British government has stated that it does not plan to withdraw from the ECHR.

It will, however, withdraw from another European institution, the Court of Justice of the European Union, which will no longer be the court of final appeal for British law. It will remain to be seen whether the ECHR will consider cases arising from serious GDPR breaches which are not decided by British courts.

The US/UK Privacy Shield

Those British companies which are transferring personal data to the US based on Privacy Shield have some good news. The US Department of Commerce has already updated the Privacy Shield with additional language (documented in the FAQ) that recognises the UK as being separate from the EU. This means the Shield may continue to be used without problems after Brexit – at least until the Court of Justice of the EU considers the Schrems II case, which challenges the use of Privacy Shield by companies such as Facebook and Google.
Recommendations for Chaucer Customers

Where you are transferring data from the EU/EEA to the UK based on a determination of adequacy, this will no longer be viable—and that will be sooner rather than later under a no-deal Brexit. Therefore, contracts you may have that rely on this adequacy will need to be updated to make use of Standard Contractual Clauses issued by the European Commission.

If you are transferring personal data from the UK/EU/EEA to the USA under the US Privacy Shield, there are some changes to the wording of the agreements that are required, which will acknowledge the new status of the UK after Brexit. As with adequacy, the effective date will differ according to whether or not there is a “no-deal” Brexit.

Where you are a business operating in a 3rd country and are processing the data of EU/EEA residents on a large scale or high-risk2 data according to GDPR Article 27, then you may require a Data Privacy Representative based within the EU. In general, your Representative should be registered in the EU Member State where the largest concentration of your data subjects is found. A separate EU Representative is however not required for each EU/EEA state, although a UK Representative may be required in addition to an EU Representative to comply with the UK Data Protection Act (2018).

As one of the key elements of GDPR is the principle of transparency, we recommend that Privacy Notices be updated where adequacy can no longer be relied upon, to explain to the data subjects which transfer mechanism (such as SCC) is now in use. The transfer mechanism itself, usually a part of a Data Processing Addendum, should be made available to data subjects upon request, such as via a website link. Best practice means that where a significant change to the Privacy Notice is made, such as lawful basis or transfer mechanisms, an effort should be made to pro-actively inform the data subjects of the changes, e.g. send a PDF copy via email to the individuals.

Naturally, any change to the transfer mechanism should

Recommendations

For Chaucer Customers

Where you are transferring data from the EU/EEA to the UK based on a determination of adequacy, this will no longer be viable—and that will be sooner rather than later under a no-deal Brexit. Therefore, contracts you may have that rely on this adequacy will need to be updated to make use of Standard Contractual Clauses issued by the European Commission.

If you are transferring personal data from the UK/EU/EEA to the USA under the US Privacy Shield, there are some changes to the wording of the agreements that are required, which will acknowledge the new status of the UK after Brexit. As with adequacy, the effective date will differ according to whether or not there is a “no-deal” Brexit.

Where you are a business operating in a 3rd country and are processing the data of EU/EEA residents on a large scale or high-risk2 data according to GDPR Article 27, then you may require a Data Privacy Representative based within the EU. In general, your Representative should be registered in the EU Member State where the largest concentration of your data subjects is found. A separate EU Representative is however not required for each EU/EEA state, although a UK Representative may be required in addition to an EU Representative to comply with the UK Data Protection Act (2018).

As one of the key elements of GDPR is the principle of transparency, we recommend that Privacy Notices be updated where adequacy can no longer be relied upon, to explain to the data subjects which transfer mechanism (such as SCC) is now in use. The transfer mechanism itself, usually a part of a Data Processing Addendum, should be made available to data subjects upon request, such as via a website link. Best practice means that where a significant change to the Privacy Notice is made, such as lawful basis or transfer mechanisms, an effort should be made to pro-actively inform the data subjects of the changes, e.g. send a PDF copy via email to the individuals.

Naturally, any change to the transfer mechanism should

Conclusion

In general, the details of data protection will be largely unchanged after Brexit, apart from a few minor areas. Adequacy is not guaranteed, or at least will be delayed during a transition period, therefore SCCs will be a good option for most small businesses dealing with the EU. Most organisations are likely to take a pragmatic approach to ensure their international transfers are lawful, which may work in the short term, but are likely to be problematic if not corrected in the medium to long term. Above all, we recommend transparency in managing your flows of personal data belonging to EU/UK/EEA residents.

If you have any questions or concerns about Data Protection and Brexit, please don’t hesitate to contact us directly, at DataPrivacy@chaucer.com, through MS Teams (if you are an existing client), or via telephone on +44 203 934 1099.