Brexit Essentials: an update on data protection and privacy

November 2017

With the United Kingdom set to withdraw from the European Union on 29 March 2019, the Ministry for Brexit faces a critical juncture for the future of data flows across Europe.

What data protection legislation will apply to the UK after Brexit?

Current EU privacy laws will be replaced in their entirety on 25 May 2018 by the General Data Protection Regulation ("GDPR"). As a result, the GDPR will apply before the UK leaves the EU. Exemptions and derogations from, and extensions to, the GDPR regime will be included in a new UK Data Protection Act. This Bill is currently before the House of Lords.

Following Brexit, if the UK stays in the EEA, the GDPR will continue to apply.

Due to its extra-territorial effect, if the UK leaves the EEA the GDPR will still continue to apply to all UK entities that do business in the EU i.e. entities offering goods or services (regardless of payment being taken) and/or monitoring the behaviours of individuals within the EU.

In any event, the UK government has signalled that the European Union (Withdrawal) Bill will incorporate the GDPR into domestic law before the UK leaves the EU. Provisions equivalent to the GDPR will therefore continue to apply in any scenario.

Key data issues

Assuming that the UK leaves the EEA, the key Brexit issue in the data privacy arena is how cross-border data flows will be permitted from the EU to the UK going forward. This is not, however, the only aspect of data privacy that is affected by Brexit. There are also important implications for transfers of data from the UK, who the lead supervisory authority for a company will be and the availability of the one-stop shop mechanism.

Key Brexit / privacy dates	
29 March 2017	Article 50 of the Lisbon Treaty is triggered
24 August 2017	UK Government publishes a future partnership paper on The Exchange and Protection of Personal Data
6 September 2017	European Commission ("Commission") publishes position paper on The Use of Data and Protection of Information Obtained or Processed before the Withdrawal Date
25 May 2018	The GDPR applies in all Member States
29 March 2019	Article 50 notice expires

Cross-border data flows

Personal data can be transferred freely between EU and EEA Member States. Personal data may only be transferred outside the EU/EEA if one of a number of conditions are satisfied. After Brexit, for personal data to be transferred from within the EU/EEA to the UK, one of these conditions will need to apply unless the UK can negotiate an alternative route. This alternative route is currently the UK Government's preferred option.

Grounds for transferring personal data out of the EU/EEA

- The Commission has made an adequacy decision in respect of the UK
- Binding Corporate Rules are in place
- Model Clauses are signed
- Approved Codes of Conduct and certifications apply
- The individuals have consented to the transfer

These options, as well as the UK Government's preferred bespoke approach, are considered below.

"Adequacy"

An adequacy decision may be granted by the Commission to non-EEA countries which provide a level of personal data protection that is "essentially equivalent" to that provided for by EU law. It can also be awarded to specified sectors of an economy or international organisations i.e. partial adequacy.

As Whitehall have been keen to point out, the UK and the EU will start from "an unprecedented point of alignment" of laws and this ought to work in the UK's favour in obtaining an adequacy decision.

"I hope that on D+1 life will continue much as on D-1, because we have taken the decision domestically to bring the GDPR into UK law."

(Matt Hancock MP, Minister of State for Digital when giving evidence to the EU Home Affairs Sub-Committee)

However, there are still potentially significant challenges.

Investigatory Powers Act 2016 ("IPA")

The greatest challenge to an adequacy decision to our mind comes from the IPA. The IPA affords UK law enforcement and intelligence agencies powers to monitor and retain certain communications data. Dubbed the "Snoopers Charter", the IPA has faced a number of challenges and received widespread criticism for failing to satisfactorily protect the privacy of individuals.

Currently, if the UK's data privacy regime were to be tested before the Court of Justice of the European Union ("CJEU"), the national security exemption under the Lisbon Treaty would be engaged. Post Brexit the UK will no longer benefit from this.

In the Tele 2 / Watson judgement, the CJEU set out guidelines on what they may consider unlawful in respect of retaining communications data. If applied to the IPA, there is a question as to whether it would fail to satisfy these. This adds

to the uncertainty as to how the Commission may view the IPA.

The result is concern as to whether the IPA will prevent the UK from obtaining an adequacy decision. The UK Government is aware of this potential issue and the Department for Digital, Culture, Media and Sport ("DCMS") has suggested that they expect to be able to justify why the IPA is proportionate and not an issue for adequacy.

Divergence in legislation

Whilst the GDPR will be incorporated into domestic law, there is a risk that interpretation will diverge over time. This may occur at the outset given that EU legislation is interpreted with a more purposive approach than UK legislation, and interpretation may in any event diverge over time. This could affect receiving an adequacy decision in the first place or could lead to such a decision being revoked in the future.

Separately, as time passes, and there are changes to EU data privacy law, will these always be incorporated into domestic law? If not, again, this risks any adequacy decision being challenged.

However, it is important to remember that the regime is based on adequacy, not uniformity. After all, other countries who have been deemed adequate achieve this by legislation that differs from the GDPR.

We are therefore of the view that this should not ultimately be an obstacle to adequacy.

CJEU

On the basis of the UK Government's position to date, it seems unlikely that the CJEU will have jurisdiction over UK businesses and institutions. Could this be taken as meaning that the UK does not provide adequate protection to the personal data of EU residents?

Again, we believe the answer is no. The point should be that EU residents should have standing before the UK courts in respect of their data issues and an effective form of redress. This approach is reflected by the fact that no other country has been required to submit itself to the jurisdiction of the CJEU in order to obtain an adequacy decision.

The power of precedent

It is interesting to note that the Commission has granted adequacy decisions for Jersey, Guernsey and the Isle of Man and their respective regimes are very similar to the UK regime. Could this make it harder for the Commission to refuse to grant the UK an adequacy decision?

Time frame

Adequacy decisions take time. The most recent adequacy decision (New Zealand) took four years.

All adequacy determinations are made in order of political expediency and the Commission has made clear the UK will need to wait its turn in the queue. Whilst the UK may ultimately receive an adequacy decision, this does beg the question as to whether it will be in place at the point of Brexit.

Assuming that the challenges of the IPA can be overcome, time is therefore the biggest challenge to adequacy. That said, the UK is a special case as there is no precedent for granting adequacy against the backdrop of the withdrawal of a Member State.

It also should be remembered that the EU will need a reciprocal adequacy decision from the UK

and so there is mutual interest in these being granted simultaneously at the point of Brexit.

Of course, if it is agreed that there will be a transitional period post Brexit, that will also assist with the timing of the adequacy decision.

Either way, we suspect that this is a case of "where there is the will there is a way".

A bespoke adequacy model

However, receiving an adequacy decision in the UK's favour is not the UK Government's preferred option. On 24 August 2017, the UK Government published a future partnership paper titled *The Exchange and Protection of Personal Data*. It put forward a proposal for a "new, deep and special partnership" between the EU and the UK. Some commentators have referred to this notion as "adequacy plus".

Whilst the proposal sets out the objectives of such a partnership (see opposite), it is light on detail. A few key points can however be deduced.

Data flows

The proposal states that there should be mutual recognition of each other's data privacy frameworks "until such time as new and more permanent arrangements come into force". This suggests an adequacy decision in the short term with it being replaced by a more bespoke arrangement down the line.

UK national security

A marker is clearly put down in this regard with the reference to the UK's ability to protect the security of its citizens. This is likely an oblique reference to the IPA discussed earlier and that the UK would not be expected to be restricted in this regard.

Objectives for a special partnership

- Maintain the free flow of information between the UK and the EU
- Offer sufficient stability and confidence to businesses, institutions and individuals
- Provide for ongoing regulatory co-operation between the EU and the UK
- Continue to protect the privacy of individuals
- Respects sovereignty, including the UK's ability to protect the security of its citizens and its ability to maintain and develop its position as a leader in data protection
- Does not impose unnecessary additional costs on businesses

Regulatory co-operation

The paper foresees an ongoing role for the Information Commissioner's Office ("ICO") and makes clear that the Information Commissioner should be allowed to retain her seat on the European Data Protection Board ("EDPB") so as to allow the UK to remain part of the regulatory dialogue.

The EDPB will be the replacement body under the GDPR for the Article 29 Working Party ("A29WP") and will consist of representatives of the national supervisory authorities. It will play a significant role in data protection compliance, with its primary function being to ensure the consistent application of the GDPR. In addition, it will

adjudicate between national supervisory authorities over cases/investigations/complaints and will issue independent and binding decisions.

Role of the CJEU?

The mention of respecting sovereignty may also be a reference to the UK Government's stated position that UK persons will not be subject to the CJEU.

One immediate challenge to the UK Government's approach is that the decisions of the EDPB amount to EU law and are subject to the jurisdiction of the CJEU. It is not therefore clear how the objectives of regulatory co-operation and respect of sovereignty are to be aligned. DCMS is aware of this issue but it is not clear how it proposes to deal with it.

The message from the Commission

The position paper published by the Commission shortly after the UK Government's paper highlights that there remains a considerable execution risk in achieving a bespoke adequacy model. The paper notes that the UK's access to networks, information systems and databases established by EU law will, as a general rule, terminate on exit.

The Commission is clear that the UK may only retain and continue to use data received and/or processed in the UK before exit if certain conditions and principles are satisfied – see box opposite. It should otherwise be deleted.

Key Commission principles

- The provisions of EU data protection law applicable on exit continue to apply
- Individuals retain their ability to enforce their rights in accordance with EU law applicable on exit
- The Withdrawal Agreement allows for the orderly completion of ongoing investigations or procedures for the monitoring of compliance with personal data protection provisions

What hope for a bespoke model?

As with other Brexit issues, the UK Government's stated position and that of the Commission appear to be at odds with each other in various key respects.

Whilst the EU has a vested interest in allowing its businesses to continue to transfer personal data seamlessly to the UK which should assist with the political will to achieve an adequacy decision, the benefits to the EU in negotiating and agreeing a bespoke model with the UK seem less clear.

Given this, it is unsurprising that the UK Government plans to run discussions regarding the bespoke model in parallel with adequacy discussions.

Alternatives

Model Clauses

Model Clauses are standard clauses approved by the Commission which if signed by the EEA data exporter and the non-EEA data importer enable the transfer of personal data between them.

There are two sets of Model Clauses approved by the Commission. One governs controller-to-controller transfers and the other governs controller-to-processor transfers. There are no Model Clauses for processor-to-processor transfers which can cause practical difficulties.

Commonly raised concerns about the Model Clauses include their restrictive nature, the difficulty and cost associated with their adoption and the fact they cannot be amended.

In addition, the future of the Model Clauses is under review by the CJEU following a reference from the Irish High Court over their validity (*Schrems II*).

The Model Clauses are popular with businesses who transfer data outside the EEA. If the CJEU rules that their use does not accord with EU data protection rules, this would have far reaching effects. Businesses would need to rely upon another basis for such transfers, further limiting the alternative options to adequacy post Brexit.

A ruling from the CJEU is expected in late 2018 at the earliest.

Binding Corporate Rules

Binding Corporate Rules ("BCRs") allow multinational companies to transfer personal data from within the EEA to their group companies outside of the EEA. A company must demonstrate its BCRs put in place adequate safeguards for protecting personal data throughout their organisation in line with the requirements of the A29WP Guidance. Putting BCRs in place takes time - the ICO estimates a straight forward application takes 12 months - and can be very costly.

If there is no adequacy or bespoke arrangement put in place, this may be a good route for many companies for internal transfers, and are particularly helpful in the context of processor-processor transfers. That said, BCRs have not generally been favoured by businesses to date and so it is more likely that Model Clauses will be the first option businesses look to.

Codes of Conduct and certifications

This new alternative under the GDPR is designed to broaden the availability of "self-regulating" methods for data transfers. The Codes may be proposed by associations or representative bodies on behalf of their industries. They are approved by a competent supervisory authority or the EDPB if more than one jurisdiction is involved. Data transfers made on the basis of a Code, together with a binding and enforceable commitment of the non-EEA company to apply appropriate safeguards, may take place without any further authorisations.

Consent

If an individual freely gives their informed and unambiguous consent to the transfer, it will be permitted under the GDPR.

However, although obtaining consent appears a neat solution to GDPR requirements, it should not be thought of as the first alternative. It may be hard to ensure that the consent is "informed"

given the information that would need to be provided before consent is given.

In addition, the concept of "freely given" can be hard to meet. This will not be satisfied if the service is conditional on consent where that consent is not "necessary" for the service, or if there is an imbalance between the parties, such as in the employee context.

There is also the perennial issue of what if consent is refused or withdrawn at a later date?

There are also challenges when dealing with existing customers given that each person would have to take affirmative action to provide their consent. Where a large consumer base is involved, the consent ground will be difficult given the acceptance rate is likely to be low.

For further information on what amounts to consent and the challenges of relying on it, see our publication on *Processing of personal data: consent and legitimate interests under the GDPR*

Restrictions on data flows from the UK

Transfers to the EU/EEA

Whilst maintaining transfers from the EU to the UK has been the main focus of concern, as mentioned earlier, a mechanism is also needed for the reverse transfer. It would however seem improbable that the UK would not decide that the EU is an adequate jurisdiction, albeit that this may get used as a negotiating card in the discussion about the UK's adequacy.

Transfers to and from non-EEA countries

Once the UK leaves the EU and EEA, the adequacy decisions adopted by the Commission in respect of other countries such as Switzerland and New Zealand will need to be adopted by the UK if existing data flows are to continue on the same basis as currently.

In addition, it will need to be considered if any data transfers are made to the UK from non-EEA countries on the basis of it being part of the EU/EEA and, if so, how those arrangements are to be replicated going forward.

The UK Government has noted that it plans to liaise with third countries to ensure that existing arrangements will be transitioned over at the point of exit.

We can also expect the ICO in due course to approve Model Clauses for transfers out of the UK, which may, at least in the short term, track the current versions approved by the Commission.

Other implications of Brexit

Identifying your lead supervisory authority

Under the GDPR, identifying a lead supervisory authority is necessary where a company is carrying out cross-border processing of personal data.

Until Brexit takes effect, the ICO will be the lead supervisory authority for companies with their main establishment in the UK. Post Brexit, unless a bespoke arrangement is agreed, the ICO will continue to be the company's regulator but, in addition, there will be a lead supervisory authority from another Member State if the company continues to fall within the scope of the GDPR.

Depending on the structure of the company in question, it may be that it will be able to flex its arrangements to be able to effectively choose its

lead supervisory authority. However, A29WP Guidelines state that the "GDPR does not permit forum shopping" – there must be an effective and real exercise of management activity in the Member State identified as the company's main establishment. A company must be able to demonstrate where decisions about data processing are taken and implemented, as they may be asked to evidence their position.

Not so "one-stop-shop"?

The one-stop-shop enforcement mechanism is only available to companies established in the EEA.

This means that companies carrying out cross-border processing will only be required to liaise with one regulatory authority. Other authorities "linked" to their processing operations, so-called "concerned authorities", may also be involved.

We understand it was a conscious decision as part of the negotiations of the text of the GDPR to limit this benefit to companies established in the EEA. For companies who are subject to the GDPR but not established in the EEA post Brexit, the benefit of the new one-stop-shop mechanism will be lost absent a bespoke arrangement being agreed which saves this.

What should companies be doing now?

The greatest risk is for transfers from the EEA to the UK – whilst the UK may wish to use a decision about whether the EEA is adequate as a negotiating card, ultimately it is within the UK Government's control to permit UK-EEA transfers.

In our view, we can be cautiously optimistic that arrangements will be put in place to enable data transfers to continue seamlessly from the EEA to the UK post Brexit, whether that be on the basis of an agreed transitional period or on the basis of adequacy. This will, in reality, depend on political will, and so the negotiations on this topic may be impacted by other parallel discussions on trade and the like.

Our advice is that there is no need to put in place contingency arrangements now. Instead we advise companies to maintain a watching brief.

As part of companies' GDPR programmes, it would be worth assessing not only where data is transferred out of the EEA but also those data flows between the EEA and the UK. Should it become clear that alternative arrangements are needed, the affected arrangements will then be easy to identify.

As part of Brexit planning, it can then be considered what alternative method would be most appropriate for each transfer. For intra-group transfers this may be Model Clauses, either as the final solution or as a stop gap until BCRs are approved. For third party organisations Model Clauses are likely to be the way forward. Given the challenges of obtaining valid consent, ideally that route would not be adopted.

Brexit Privacy Checklist

- Assess data flows between the UK and EEA
- Consider the most appropriate alternative method of transfer for each data flow
- Maintain a watching brief (and be ready to spring into action if needs be)

This article was written by Rebecca Cousin and Chloe Halloran.

If you have any queries on this Briefing or if you would like to discuss any aspect of the GDPR or any data protection or privacy issue, please contact Rebecca Cousin, Rob Sumroy or your usual Slaughter and May contact. Further publications are available on our website.

Rebecca Cousin
T +44 (0)20 7090 4738
E rebecca.cousin@slaughterandmay.com

Chloe Halloran
T +44 (0)20 7090 3871
E: chloe.halloran@slaughterandmay.com