Brexit Q&A

Data Protection

In another of our Brexit Q&A series, Anna Drozd, EU policy adviser and Kirsty Fryer, trainee solicitor with MacRoberts on secondment at the joint UK law societies Brussels Office, answer some questions you might have about the things you will need to take into account in respect of data transfer and protection after the end of the transition period on 31 December 2020.

Q: Hi Anna and Kirsty. Thank you for answering our questions. First of all, what has the Brussels Office been doing since the UK voted to leave the EU?

A & K: Hello and many thanks for having us. Our office has indeed been quite busy over the past four years. First of all, we were focused on helping our members. Many of them had questions about the impact of Brexit on their career and the future of their firm. Secondly, many members were concerned about the impact of Brexit on their key areas of practice, such as judicial cooperation on civil and commercial matters, family law, data protection, intellectual property, etc. So, we were also busy with providing advice on these areas of law. Thirdly, we represented members towards the UK Government and EU institutions in order to flag any areas of concern from our profession. This work with the EU and UK negotiators together with other stakeholders in Brussels allows us to also have intelligence that we share with our members about the negotiations.

Q: Why is cross-border data protection with the EU currently something we need to think about?

K: Well, simply put, we need to be thinking about our cross-border data protection with the EU now because once we leave the EU, we will become a “third country” and, in the situation where there is no adequacy decision, we will be required to put additional protective measures in place in order to safely transfer data across jurisdictions. In today’s world, data is at the centre of everything we do – a business cannot operate without processing personal data – it is therefore hugely important that every UK business is prepared for the upcoming changes.

As some readers may know, the UK government are currently seeking adequacy decisions with the European Commission which, if granted, will allow data to flow freely between jurisdictions – in the same way that it does now. The European Commission will only grant an adequacy decision if they are satisfied a third country has an adequate level of data protection. As the UK has been subject to the EU’s GDPR since its inception, and the UK Government has confirmed they will not radically change UK data protection laws following Brexit, it is likely the European Commission will grant an adequacy decision to the UK. It is important to bear in mind, however, that this is not a foregone conclusion; especially as the EU has recently expressed concern regarding UK surveillance laws and its relationship with the US.

Should the European Commission refuse to grant an adequacy decision to the UK, any cross-border data transfers with the EU will take place within the framework of additional safeguards (under Article 46 of the GDPR).

Considering the many moving parts and variety of possible outcomes, it is hugely important for businesses (including law firms) to be prepared for the changes about to take place BEFORE the end of the transition period. By thinking about cross-border data protection with the EU now, businesses should be able to put the appropriate mechanisms in place before the end of the year, which in turn, will allow their personal data to flow freely following Brexit.

Contact: Katie Hay, Head of International | Tel: 0131 476 8351 | Email: katiehay@lawscot.org.uk

Q: What sorts of things that I currently do might be affected by this change?

K: This is a great question and one that has many possible answers! In respect of law firms, the undernoted provides just a few examples of things that will be affected by the change:

- If the firm has offices in both the UK and Europe, then the simple sharing of a firm-wide intranet would constitute a cross-border transfer of personal data.
- As firms are now required to be far more diligent in respect of AML regulations and 'Know Your Client' procedures, it is likely firms will hold client data which is of a cross-border nature.
- Human Resources may hold data in relation to EU national employees.

It is important to bear in mind, however, that every business is different. It's highly likely that they will have their own bespoke IT systems. It is for this reason it is so important that every organisation looks at their own set-up, as soon as possible, and has real think about the types of data they hold and process during their ordinary course of business. Once they have had a think about it, they will know if they need help – and it's always better to ask for help sooner rather than later!

Q: But we implemented the General Data Protection Regulation so why will things be different?

A: The UK will become a third country. This means it will not be part of the institutional network which helps make sure the GDPR is respected. Also, every piece of legislation evolves over time. There may be changes in how it is interpreted and applied in the EU and in the UK. For example, the Court of Justice of the EU (CJEU) can issue judgments on the same issue as the UK courts but with a different result. Also, EU data protection authorities may issue different guidance than the ICO.

Over time, these differences can become quite important. So, to make sure that personal data outside of the EU has the same protection that the EU law, the European Commission conducts an assessment. If it is positive, the Commission adopts an adequacy decision and the data flows can continue as they do now.

The situation changes if the assessment is negative. In such a case, organisations that transfer personal data from the EU to the UK must take extra steps to follow the law.

At the moment, the Commission is busy with drafting two adequacy decisions. One is under the GDPR and another under the Law Enforcement Directive. We invited techUK to share their views on the process with us and you can read it here.

For now, we need to wait and see what the result will be. Yet, there are some steps that everyone can take to get ready regardless of the result.

Q: Can you tell us more about these steps?

A: Of course. You should begin with a review of your data flows to see if you receive personal data from contacts or clients in the EU. If you do, there are several steps you should follow. To a certain extent, these will depend on your business operations. For example, if you are a small or medium-sized firm, you should use the Information Commissioner's Office (ICO) interactive tool to decide what action to take.

First of all, you should see what transfer mechanisms you use. At the moment, you have several options under the GDPR:

- standard contractual clauses (SCCs);
- binding corporate rules (BCRs);

- codes of conduct and certification schemes;
- derogations.

In practice, the SCCs are probably the most popular mechanism. There three different types of the SCCs and all are available here. You must remember that to use the SCCs, data exporters and importers have to carry out a risk assessment. It is to make sure that they provide sufficient protection within the local legal framework. This requirement is a result of the recent case before the CJEU (see here for background). There are guidance notes that can help you carry out such an assessment and are available here and here. The ICO is yet to publish its guidance.

Secondly, you should review your privacy policies so that your clients understand the movement of their data.

Thirdly, you should consider appointing an EU representative if you have not done so already.

Fourthly, you should check your website and information society providers. This is because some of these services may have to stop after the end of the transition period. For example, there are rules on the use of the .eu domain. You can check the official Government guidance here.

Finally, you should be aware of the existing guidance and advice and whether it is updated. There are already many sources that are being updated and it is worth checking regularly.

Q: Could you give us some hints as to where we should look for further information? / Where should I look for further information on things like standard contractual clauses?

K: The ICO really should be your first port of call. The ICO (which stands for Information Commissioner's Office) is the UK's independent authority set up to uphold information rights. They have offices across the UK, including Scotland.

The ICO have a great range of online materials to consult when preparing for the upcoming change – including a specific guidance on the end of the transition period. They also have a contact page which provides email addresses and phone numbers for those questions which are that bit more technical, or for those organisations that would prefer to discuss any worries or concerns with an expert.

You should also regularly visit the website of the Law Society of Scotland for all latest updates.

You can also check the official UK Government guidance on data protection after the end of the transition period, European Commission guidance and European Data Protection Board (EDPB) guidance.

The UK Law Societies (and the Brussels Office) will continue to publish guidance – keep an eye out for each society's respective posts.

Q: Do you have any other advice to offer?

A: I think that the main piece of advice from me would be to dedicate enough resources to getting prepared. There are a lot of resources already available, but it takes time to review business processes related to data protection and cross-border transfers.