Slaughter and May Podcast

Beyond adequacy - Brexit's wider data privacy implications

Rebecca Cousin	Hello I am Rebecca Cousin, Co-Head of our Data Privacy Practice and I am joined today by Cindy Knott, Head of Data Privacy Knowledge. With the Brexit transition period ending on 31 December it's time, if you haven't already, to refocus on Brexit planning. Whilst it has been a topic of international transfers that has received the most coverage in the data privacy context, there are other aspects too that need to be considered. So in this session Cindy and I are going to recover a number of these as well as international transfers. Firstly it is worth me explaining the legislative framework. As you will know the main privacy law in the EU is the general data protection regulation referred to as the GDPR. With effect from 1 January 2021, the UK will write the GDPR into domestic law for the few minor tweaks, for instance replacing references to EU bodies with the equivalent to the UK ones. We will therefore technically have the EU GDPR and the UK GDPR. With that background out of the way Cindy could you explain when each regime applies?
Cindy Knott	Of course. So obviously if you are based in the EU, the EU GDPR will apply to you, and likewise if you are in the UK, the UK GDPR will apply. It's also pretty well known that the EU GDPR has extra territorial effect and so will apply to non-EU businesses either offering goods or services to people in the EU or monitoring their behaviour whilst in the EU. The UK GDPR being essentially a copy out of the EU GDPR also has extra territorial effect on the same basis. A UK business could therefore be subject [as opposed] to UK GDPR and the EU GDPR. However that is not the end of the story, as under the EU withdrawal agreement the EU GDPR will continue to apply to personal data of non-UK persons which was processed in the UK under the GDPR during the transition period. This provision only applies unless and until the UK obtains an adequacy decision from the EU. We will come back to adequacy later but given the current uncertainty here this provision is likely to be relevant to a significant number of businesses so for example, those that have a centralised HR function in the UK which processes personal data about employees in other countries, or those that have customers whether corporate or individuals outside the UK.
Rebecca Cousin	Cindy that is a really good point and one that is easy to miss. But what do you think companies should be doing about this?

Cindy Knott	In the short term, while the data privacy resumes area aligned there will be few practical implications where by regimes apply to either of the reasons I have just mentioned given the requirements will be the same under both. And so really from a day to day perspective we expect companies to continue to have one compliance programme. One point to note however is that if a company is based in one jurisdiction and is caught by the extra-territorial provisions of the other regime, then it needs to have appointed a representative in that jurisdiction. For non-EU businesses that already have a representative in the EU or the UK, they will also likewise need to consider if they need to appoint a second in the other jurisdiction. And then finally the other point worth noting is that in a breach perspective, if they were to be a data breach in respect of data that is subject to both regimes the notification to data protection authorities under both regimes would be required.
Rebecca Cousin	Yes that is a good point again because, and of course this reflects that businesses that become subject to both the EU and the UK GDPR will run the risk of being fined under both regimes for the same breach. I mean of course this is no different to the existing position regarding global investigations where a business may be sanctioned, for instance, in the US and the EU for the same incident but the size of the possible penalties and the context of the EU and UK GDPR up to 4% of global turnover in each case, is far higher raising the risk profile and potentially shifting the balance on risk assessments. I think on the subject of enforcement many businesses have to date benefited from the one-stop shop mechanism. This meant that businesses had one lead EU data policy regulator who would bring enforcement acts in for the whole of the EU. However unless you can show that you have a so-called main establishment in the EU after Brexit, this will cess to be available. Not only would you therefore be subject UK and EU enforcement but multiple regulators in the EU could in theory at least bring enforcement action. It's therefore important to assess whether you do have a main establishment in the EU, and so identify your new lead supervising authority. The involvement of different regulators and enforcement to those to which a business is currently subject does also change the risk profile due to different interpretations regulating priorities and approaches to enforcement. For example, while the ICO's enforcement action has primarily focused on data security to date, with it now having issued three signs under the GDPR the Spanish regulator has taken action in respect of a much broader range of matters with over 120 fines having being issued. If a different regulator therefore has jurisdiction post Brexit this will change the risk profile of the different processing activities, and it is worth reviewing previous risk based decisions to ensure that they still stand in the light of a changed regulatory context.

	One area of potential divergence going forward in enforcement approach may be in the area of international transfers. There has been much movement on this recently. Cindy could you explain the latest position on international transfers?
Cindy Knott	Thanks Rebecca. So the concern here has been to ensure that data can continue to flow freely from the EU to the UK and vice versa. The reason for this concern being of course that under the EU GDPR there are restrictions on personal data leaving the EU. The UK GDPR contains identical restrictions but in this case applying to transfer to jurisdictions outside the UK. The aspect that is received most focus has been whether the UK will receive what is referred to as an adequacy decision from the EU. That is basically a decision that the UK provides an essentially equivalent level of protection to personal data so that such data can continue to flow freely. For transfers from the UK to the EU, the UK government has helpfully confirmed that this can continue to flow on the basis of a temporary adequacy decision in respect of the EEA countries. However the position to transfer from the EU to the UK is still unclear. Given where we are in a year a decision from the EU by the end of December is looking increasingly unlikely, but you might wonder what the issue is here given that the UK with have no identical privacy legislation but the answer to that is in addition to the data privacy legislation in itself, the UK government surveillance laws also need to be considered by the EU.
Rebecca Cousin	So Cindy, given the current position what would you advise organisations to be doing now?
Cindy Knott	Well I think we have to assume that there won't be an adequacy decision in time, so organisations should identify now if there is another basis under the GDPR for their transfers. Obviously the first step is going to identify which data flows are affected and then to assess which of the other options under the EU GDPR is the most appropriate. Some of the transfers may fall under the so called derogations but these are narrow categories for occasional transfers and so really the majority of data flows won't meet these requirements. Instead, for most organisations the answer will be to put in place the standard contractual clauses between the EU entity and the UK recipient. These being the contractual provisions approved by the EU for this very purpose. But of course there has been Strems two cases which made the headlines this year. Rebecca, how does this case impact with the approach?
Rebecca Cousin	Yes there definitely is a change following that. The case upheld the validity of the standard contractual clauses very helpfully, but additional sets are now required with there being an obligation on the EU entity which wishes to transfer the personal data to undertake an assessment of the regime in the UK, as with any other non-EU country to determine if the standard contractual clauses would provide sufficient protection in the circumstances.

	The European Protection Board, the group of all EU data protection authorities has recently issued guidance setting out the factors they consider should be taken into account in this assessment, and suggesting additional steps that could be taken if that initial assessment suggests that the standard contractual clauses are not within themselves at least, sufficient to provide the required level of protection. This assessment will also therefore need to be factored into organisations Brexit planning just in the same way as any other international transfer. But of course it doesn't end here Cindy because of course the EU commission is now consulting on updated standard contractual clauses so what is the impact of that?
Cindy Knott	They are no enforced yet. They are still in draft, so I agree they are unlikely to be enforced before the end of the year in fact and organisations should therefore proceed with putting in place the existing standard contractual clauses. They should also however put in place a process for entering into new clauses no later than a year after the new ones come into force.
Rebecca Cousin	Thanks, one other thing I did want to mention is the potential need to change the processing ground that organisations are relying on. This most obviously arises where special category data is being processed given that the processing grounds for these are in the main set out in national legislation. If processing special category data in the UK, where that data is also subject to the EU GDPR the relevant processing ground under the EU GDPR will therefore have to be assessed as well. It can also arise for other personal data where the processing ground relied upon, is where the processing is necessary to comply with a legal obligation under EU or member state law. Obviously from January that is not going to include the UK, so if an EU business is relying upon a UK law that will fulfil this legal obligation basis. It is going to need to identify a different ground most likely the legitimate interest ground. This change would then need to be reflected in amendments to records of processing, privacy notices and other internal documentation. Cindy was there anything else you wanted to raise?
Cindy Knott	One quick thing I wanted to mention is processor terms. The mandatory requirements for processor terms under the EU GDPR refer in a number of places to EU or member state law. In the UK GDPR this has been changed to refer to UK domestic law. This will therefore need to be reflected in the drafting of these provisions. Whilst we don't envisage that there will be any desire in practice to amend existing agreements, companies should at least be factoring this in for the drafting of new contracts.
Rebecca Cousin	Good point. Thanks Cindy. Well that brings us to the end of what was a very quick overview of a few of the key Brexit planning areas for data privacy. There is more detail on each these and other areas in our recent article *Beyond Adequacy: Brexit wider data policy implications* which you can find on our website. Thank you.