Brexit Institute
17th October 2019
DCU Alpha
Text of address by Helen Dixon, Irish Data Commissioner

INTRODUCTION

Thanks to the DCU Brexit Institute for the invitation to be here today. It's an extra pleasure for me that the institute is joined today by my former colleague on what was the Article 29 Working Party in Brussels, Peter Hustinx, a person who is invariably credited with having brought data protection to the top tier of the EU agenda.

I first came across the DCU Brexit Institute when I was speaking roughly this time last year at a data protection conference called Bitkom in Berlin and the Irish Ambassador in Berlin kindly invited me to an evening event at the Irish Embassy while I was there which was a DCU Brexit Institute debate on the Future of European Foreign Policy. And it was a fascinating and insightful discussion and one which highlighted the particular risks for security arising with any loss of UK intelligence data-sharing with the wider EU. So it is no surprise me to me that the DCU Brexit Institute is very much alive to the issues of both free flows of personal data and data protection.

And, of course, the data issues and in particular the personal data issues that arise with the UK's departure from the EU are non-trivial and are both broad and deep. Personal data is involved in everyday transactions between the UK and Ireland including on the island of Ireland between North and South in the context of Immigration and Asylum, Law Enforcement, Security and Intelligence, all sorts of Trade and Commerce, Banking, Medicine, Sports Administration, Tax, Tourism and so on. And up to now, we've simply never had to think about jurisdictional implications when personal data flows from Ireland to the UK including Northern Ireland and vice versa as EU data protection law guarantees free flows of personal data within the EU and in fact the broader EEA.

MANY FACETS TO THE DATA PROTECTION AND DATA FREE FLOW ISSUES

There are many facets to the issues of Brexit and data protection and including for example the impact on the European Data Protection Board of losing the contribution of the Information Commissioner's Office in the UK, the impact for the Irish Data Protection Commission in terms of the UK falling outside the One-Stop-Shop provisions in the GDPR and the loss of our main common law colleague at EU level. In addition, it's also interesting to think about the angle of the ultimate effects on innovation in the UK of being outside what some refer to as constraints of the GDPR and CJEU case law – this idea that the GDPR stifles innovation. But for today, I think my comments will *mostly* focus on personal data transfers as this is by far the area of most significant and widespread impact of Brexit on data protection. For those in the audience who are not data protection experts, legal safeguards for personal data transfers is quite a terminology-laden area. I won't go too far into it and will keep it quite high level and I think you will get the gist of it.

I think everyone here is likely familiar with the fact that while EU data protection law guarantees free flows of personal data within the EEA, it conversely prohibits transfers of EU personal data outside of the EEA unless it can be demonstrably ensured that the level of protection guaranteed by EU law is not undermined. In other words, it would be pointless to have strong laws to protect our personal data in the EU if an organisation could simply bypass those laws by easily transferring our personal data to a jurisdiction with lower protections guaranteed. And therefore when the UK departs the EU, automatically guaranteed free flows of data will exist no longer. It's almost a little difficult to imagine. Because transfers occur as I said earlier in all sorts of sectors and scenarios but in very everyday ways – for example, if an organisation in Dundalk uses an outsourced payroll provider that's based in Newry

or uses AWS cloud storage in the UK, these will all count as transfers of personal data to a third country post Brexit.

HOW TO LAWFULLY UNDERPIN DATA TRANSFERS ONCE FREE FLOWS ELIMINATED

The means by which it can legally be demonstrated that EU protections are not being undermined in transfer scenarios outside the EEA are multiple: firstly, the EU can recognise a third country, territory or sector as providing an adequate level of protection. Only 11 countries in the world have been recognised as adequate for this purpose so far by the EU in addition to two partial adequacy findings in respect of Canada and the US. Negotiations are complex and therefore slow in each case because they require the EU Commission to make a complete assessment of the laws, practices and international commitments of any country under assessment that would affect data protection. The CJEU has pointed out that adequacy does not require a third country to have an identical system of protections but there must be what it calls "essential equivalence" and equally the CJEU has confirmed that a finding of adequacy cannot be static. It must be kept under review every couple of years by the EU Commission to ensure there has been no material change in circumstances. The GDPR now builds in this review period requiring it be conducted at least every four years and to take into account all relevant developments in the third country. So, even in a "with deal" scenario, it has to be said that there is no guarantee that by the time the transition period at the end of 2020 concludes that an adequacy finding would be in place in respect of the UK both in terms of the short time left to conclude such an agreement (they've generally taken years for other jurisdictions), in terms of the substance of what would fall to be analysed in such an assessment and in the context of the somewhat political nature of adequacy negotiations. In addition, the more frequent review periods for adequacy findings meaning they are not the "forever" option many once viewed them as and many of the existing countries with adequacy facing into being reviewed by the EU Commission over the next year are nervous about holding onto their adequacy status.

I've heard arguments from UK counterparts that the UK simply shouldn't fall to be assessed in the way other third countries are - given that just yesterday it will have been part of the EU free-flows and that it will operate a law that is effectively the UK version of GDPR mirroring the EU provisions. Their argument is that there should be an automatic awarding of adequacy to the UK without the need for lengthy assessment. While I can see where this argument comes from, this view doesn't appear to reflect legal or political reality. Nor does it consider, for example, the fact that the UK would not be subject to the jurisdiction of the Court of Justice of the European Union which plays a significant role in interpreting EU data protection law and against a backdrop of the EU Charter of Fundamental Rights to which the UK would no longer be a party. So essentially, I would point out that a "with deal" Brexit from a data protection point of view gives us the breathing space of another 14 months of data free flows during the transition period but the period from 2021 onwards would remain far from certain.

In the absence of adequacy, other means that can be used to demonstrate appropriate safeguards are in place for transfers are Standard Data Protection Clauses approved by the EU Commission to be used in private contracts between the data exporter and importer. For third countries to the EU currently, these are the most frequent and commonly used legal mechanism to effect transfers. In theory, in most cases, contracts should already be in place in the context of Article 26 or Article 28 of the GDPR which require organisations sharing data as joint controllers or in a controller to processor relationship to have written contracts in place detailing their responsibilities. And this applies even within the same jurisdiction. So, if a company in Dublin today outsources the processing of its payroll to another company in Dublin, it would have a written article 28 GDPR contract in place to define the parameters of the processing and similarly if the outsourced provider of payroll services was in London, there would be an article 28 processing contract in place between the company in Dublin and the entity in London. And so these Standard Contractual Clauses for transfers that I referenced should in that latter

case simply slot into the existing article 28 processing contract. At least that's the theory. In talks we have given in the context of Brexit, we meet blank faces sometimes when we talk about the Article 28 contracts that should anyway be in place so it may beg the question of what compliance levels with that provision are currently.

And I'm going to come back to this mechanism in a while to talk about the Irish DPC high court application for a reference to the CJEU on the validity of these clauses and where that is going. For intra-group transfers of a global corporate, so-called binding corporate rules can also be used to implement and demonstrate sufficient safeguards with enforceable data subject rights for transfers between establishments in the group. In addition, a range of very narrow essentially once-off derogations may be used but which are not suitable for ongoing structural transfers. I should mention also that the GDPR provides for additional new transfer options based on codes of conduct and certifications but these are not operational at this point in addition to which Article 46 provides for legally binding and enforceable instruments between public authorities.

NO-DEAL SCENARIO

So, in a no-deal scenario then, the UK moves overnight to third country status plus there will be no adequacy finding in place and therefore Standard Data Protection Clauses, Binding Corporate Rules, appropriate instruments between public authorities, etc. will need to be in place in respect of all personal data transfers which are as I outlined earlier an everyday occurrence. The Irish DPC has been working hard over the last number of months to prepare public sector bodies and SMEs in particular for the new and immediate requirements in the event of a no-deal. We've published detailed guidance including a set of Standard Contractual Clauses with a detailed explanatory memo to help organisations implement these legal safeguards without necessarily having recourse to legal services. We've participated in multiple webinars, worked with industry representative bodies, spoken at conferences, roundtables to push our guidance and awareness of the requirements out. We've hooked ourselves into the Government of Ireland initiative on its gov.ie/Brexit website to ensure data protection requirements are prominently detailed. We've approved, or are in the process of reviewing, schemes under Article 46(3)(a) for 6 Government Departments and the Road Safety Authority.

So while it's hard to have visibility without commissioning a focussed survey, we estimate there is a reasonable level of awareness and some preparedness in Ireland around these data transfer issues, particularly in a public sector and law enforcement context.

ON THE UK SIDE

On the UK side, our UK counterpart, the Information Commissioner's Office has published very detailed guidance for all types of organisations. It clarifies that a new UK GDPR law, once the UK exits, will permit data free flows from the UK to the EEA. The UK will also recognise the existing adequacy findings of the EU Commission for third countries and transfer mechanisms that I outlined earlier in respect of UK businesses transferring to for example the USA. The UK guidance strongly encourages all UK organisations that currently receive personal data from EEA based organisations including in Ireland to liaise with the personal data exporters in Ireland or elsewhere in the EEA to ensure Standard Contractual Clauses are inserted into contracts between them in order to legally underpin the personal data transfers. In addition, the ICO reminds UK businesses that if they are targeting EU users with their goods and services and don't have any establishments of their business in EU member states, they will need to appoint a representative under Article 27 GDPR in an EU member state.

In fact, one phenomenon we have seen is that several large scale companies headquartered in the UK have moved their EU main establishment and their Binding Corporate Rules to be supervised by the

DPC in Ireland to avoid a scenario where they are sitting outside the EU for the purposes of OneStop-Shop. This has represented a fairly significant increase in workload for our data transfers team but we understand the reasons why companies have sought to make this move.

So the issues of data transfers are significant and pervasive and require action from many organisations in the case of a no-deal. In the case of a with-deal, we have a 14-month reprieve but the transfer requirements may kick in after that transition period if for any number of reasons adequacy negotiations between the UK and EU have not been concluded.

STANDARD CONTRACTUAL CLAUSES

Before moving on from the subject of personal data transfers once the UK in whatever form departs the EU, let me come back to that issue I mentioned earlier of the Irish DPC application to the High Court in relation to the validity of EU-approved Standard Contractual Clauses. I mentioned earlier that once the UK departs, in the absence of an adequacy finding, the most convenient and frequently used method to legally effect personal data transfers will be via Standard Contractual Clauses which have been approved for use by the EU Commission. This mechanism has been used by Facebook and many other companies to transfer personal data from their EU operations to their US headquarters. On foot of a complaint from an Austrian national, Max Schrems, to the effect that his fundamental rights were breached arising from Facebook's transfers from Ireland to the USA given the potential outlined in Snowden's disclosures for NSA or US intelligence access to EU personal data, the Irish DPC examined whether what is contained in the EU Standard Clauses can ensure in its safeguards that EU fundamental rights are protected. In particular, the Irish DPC identified that nothing in these private contracts could remedy any deficiency in a third country system and, that in the context of the USA, the article 47 EU Charter right to an effective judicial remedy if an individual had a concern that their personal data had been unlawfully accessed by US authorities was not protected. We therefore implemented what the CJEU directed us to do in its Schrems judgement of October 2015 and we engaged in proceedings before our national courts in order to seek a reference to the CJEU so that it could decide if the binding legal EU instrument finding these clauses adequate in terms of the safeguards they offer are valid. Until the CJEU makes a finding of invalidity, if that's what it chose to do, these clauses remain valid and operable. There are any number of potential outcomes to that litigation (for example, the CJEU might find the clauses are valid) and equally the CJEU may decide the issues specifically in the context of transfers to the USA. So, it's reasonable to say there is a significant question mark over Standard Contractual Clauses but there's nothing any of us can do about that – they are the legal mechanism currently available and if the CJEU ultimately makes a strike-down impacting their use that bridge will have to be crossed at the time. The Advocate General's opinion in that case is due to issue on 12 December 2019 and we would expect the judgement of the Court will follow shortly thereafter.

ENFORCEMENT

Finally, the question arises as to what the consequences are if there is a failure to comply with the new requirements for legal underpinning of personal data transfers post the UK departure from the EU. Some have questioned if there will be significant effects in areas where transfers and data freeflows grind to a halt. It is possible that some organisations will refuse to make transfers from the EU if they are unable to put the necessary contractual arrangements in place with the UK recipient of the data and it would be remain to be seen what the consequences of this are.

In other cases, undoubtedly organisations will continue to transfer personal data and will fail to implement the required legal safeguards that I've talked about today. This is a big risk to take. Firstly,

individuals whose personal data is transferred may make a complaint to the DPC bringing the noncompliance to our attention. Equally individuals who consider their rights have been adversely affected by a transfer unlawfully executed may seek compensation in court if they can demonstrate that they have suffered material or non-material damage. Equally, if a data breach occurred, this could bring the unlawful transfers to the attention of individuals and the data protection authority and the fines under the GDPR for non-compliance is at the large end – up to €20m or 4% of the turnover for the preceding year of an undertaking. So, while I realise, organisations have so much to deal with surrounding changes that arise with Brexit, this is an area of compliance ignored at your peril.

OTHER ISSUES

Let me move on then from the challenging topic of personal data transfers and look at a few of those other perhaps more minor issues I mentioned.

And I'll start with an issue close to the heart of the Irish DPC. Whether with deal or without, the UK's departure from the EU means that the Information Commissioner's Office in the UK will no longer be part of the EU decision-making body, the European Data Protection Board or EDPB. The EDPB is a big part of the Irish DPC's life. We participate at monthly 2-day plenary meetings of the board and each week multiples of our staff are participating in various expert subgroups of the Board all in Brussels. Given our respective common law backgrounds and daily spoken language of English, in addition to our shared pragmatic approach to data protection issues, the ICO and the Irish DPC are close colleagues. We will feel their absence generally and the absence of their contribution and expertise around the table. In addition, it means that the One-Stop-Shop for data protection at EU level comes slightly asunder in that multinational companies with establishments in the UK and elsewhere in the EU will no longer be subject to the jurisdiction of just one lead supervisory authority but rather will now be subject to the lead authority in the EU but separately to the ICO in the UK**.**

We hope to overcome the issue of duplicated regulation and enforcement by working closely with our UK colleagues on their departure through the various other international fora for data protection cooperation in which we participate. Of course, it does mean in time we could end up with contradictory interpretations of the GDPR and the UK GDPR mirror law as the UK sits outside the EU cooperation and consistency mechanism and will not be subject to CJEU jurisdiction.

Another issue that the Irish DPC is watching with interest is the matter of the technological solutions to customs and people checks at whatever borders that are established at once the UK departs. We've heard discussions of gps and phone tracking of transport vehicles and these types of issues would have to be looked at to ensure data protection compliance in their implementation.

Finally, it's worth mentioning that sometimes with the bad press the GDPR gets – much of it unwarranted and reflective of poor and incorrect implementation – there has been speculation that it inhibits EU innovation and will strangle fledgling artificial intelligence indigenous innovation including in areas like connected cars and smart homes type applications. It will be interesting to monitor what happens over time with the UK GDPR mirror law. Will it get watered down? Will it become more flexible than EU law? Will the lack of CJEU jurisdiction allow different types of application of the law? Will there be a measurable difference in terms of attracting and supporting data-fuelled innovation in the UK versus the EU? I don't expect there will be even if the UK law starts to diverge. The GDPR is simply a set of principles that prescribes the correct way to go about lawful and fair use of people's personal data. And that's a win-win in our book.