GDPR in the UK after Brexit and Geopolitical Discrimination in Enforcement of Regulatory Sanctions

The General Data Protection Regulation ("GDPR") has heralded a new era in the protection of personal data. Individuals are now much more aware of their rights in relation to their personal data and, given the potential eye-watering fines for non-compliance, those that process personal data are now much more aware of, and compliant with, their obligations and responsibilities.

The introduction of the GDPR in May 2018 was a watershed moment, signalling the awakening of the realisation of the intrinsic value of data, and personal data in particular. Personal data is now truly understood to be a commodity and, around the world, the GDPR and the protection it affords is seen as the gold standard and something to aspire to and emulate.

What, then, will happen to the GDPR and the protection of personal data in the UK following Brexit?

The GDPR As Retained EU Law

The European Union (Withdrawal) Act 2018 (as amended by the European Union (Withdrawal Agreement) Act 2020) provides that any direct EU legislation (which includes EU Regulations such as the GDPR) operative immediately before "IP completion day" (11:00pm on 31 December 2020 – i.e. Brexit) will form part of domestic law after Brexit as "retained EU law".

Therefore, the GDPR will become part of the UK's domestic law following Brexit ("the Retained GDPR").

The UK GDPR

However, the Retained GDPR will contain deficiencies arising out of the UK's exit from the EU, either because provisions relate to reciprocal arrangements, are otherwise redundant due to the exit from the EU or because there are references to EU instruments which are no longer appropriate.

The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 ("the 2019 Regulations"), which come into force at 11:00pm on 31 December 2020, amend the Retained GDPR for a domestic UK context. They correct any deficiencies and ensure that the law continues to function effectively following the implementation period. For example, by amending the EU language to domestic language, transferring functions conferred on the European Commission by the GDPR to the Secretary of State and/or the Information Commissioner, and omitting the provisions regarding cooperation and consistency between Member States.

The 2019 Regulations will further amend the Retained GDPR so that it also includes the regime as established by Chapter 3 of Part 2 of the Data Protection Act 2018 ("DPA 2018"), which is currently outside the scope of the GDPR.

Thus the 2019 Regulations create a new single regime: the UK GDPR.

Will the UK GDPR Differ from the EU GDPR?

For the most part, other than the 'domestication' of the provisions, the UK GDPR will remain the same as the EU GDPR, imposing the same obligations on data controllers and processors, and providing the same rights for data subjects.

However, the one substantive, and practically and politically problematic, difference between the UK GDPR and the EU GDPR will be the rules relating to the transfer of personal data to third countries or international organisations. Prior to Brexit, every country and organisation outside the EU/EEA constituted a third country or international organisation but, following Brexit, every country outside the UK (including EU/EEA countries) will be a third country or international organisation under the UK GDPR, and the UK will be a third country in respect of the EU GDPR.

How, then, will the cross-border transfer of personal data be regulated after Brexit?

Cross-Border Transfers of Personal Data Following Brexit

Data is said to transcend the physical and remove all borders and barriers; and, given the ease with which data can be transferred to anywhere in the world at the click of a button, one might hope that the regulation of cross-border transfers of personal data would be a relatively straightforward matter.

This is not, however, the case. The cross-border transfer of data is hugely regulated - it constitutes an entire chapter in the GDPR (both the UK GDPR and the EU GDPR) - and can become a highly technical debate - if data is stored in “the cloud”, when does accessing it, downloading it, viewing it etc. constitute a cross-border transfer of data? If data is transferred from a country to its embassy overseas, does that constitute a cross-border transfer of data? (see *Johnson v Secretary of State for the Home Department* [2020] EWCA Civ 1032)

And the regulation of cross-border transfers of personal data is only going to become more complicated, and political, following Brexit.

The Decision Makers

As the European Commission will no longer have competence in relation to the regulation of personal data in the UK after Brexit, its powers in respect of making adequacy decisions are to be transferred to the Secretary of State. Therefore, the Secretary of State will be able, through 'adequacy regulations', to specify that a third country, territory, sector or international organisation (i.e. anything outside the UK) ensures an adequate level of protection of personal data so that transfers of personal data may be made to them without further authorisation. The Secretary of State will be required to consult the Information Commissioner before making an adequacy regulation.

The Secretary of State and/or the Information Commissioner will also have the power to specify or issue (respectively) standard data protection clauses.

UK-EU/EEA Transfers of Personal Data

As indicated above, due to the fact that the UK GDPR will be UK specific, all EU Member States, EEA countries, EU/EEA Institutions and Gibraltar will constitute third countries and international organisations following Brexit. The 2019 Regulations, therefore, provide transitional arrangements in the DPA 2018 for the continued transfer of personal data to these territories and international organisations by deeming them as having been specified in Secretary of State adequacy regulations.

Therefore, the transfer of personal data from the UK to EU/EEA countries and organisations can continue seamlessly after Brexit.

EU/EEA-UK Transfers of Personal Data

Following Brexit, the UK and its institutions will be a third country and international organisations for the purposes of Chapter 5 of the EU GDPR. Therefore, even though personal data can continue to be transferred seamlessly from the UK to the EU/EEA, the same is not true for transfers from the EU/EEA to the UK.

Transfers of personal data from the EU/EEA to third countries and international organisations can only take place if:

- there is a European Commission adequacy decision in place;
- the data controller or data processor has provided appropriate safeguards, and enforceable data subject rights and effective legal remedies for data subjects are available;
- binding corporate rules are in place;
- the sender and recipient of personal data have entered into a contract that incorporates standard data protection clauses; or
- one of the derogations outlined in Article 49 applies.

The UK would, ideally, have an adequacy decision in place, as that would mean the continued transfer of personal data from the EU/EEA to the UK without any specific authorisation. However, no adequacy decision is currently in place for the UK and, unless and until one is, transfers to the UK from the EU/EEA will only be able to take place under one of the other mechanisms. These other mechanisms are likely to require a significant amount of legal input, time and expense in advance of the personal data transfer, which may not be a viable option for everyone, and may make the UK a less attractive place to do business.

In terms of the UK being granted an adequacy decision, for a country to be granted an adequacy decision under the EU GDPR, the country in question must ensure an adequate level of protection i.e. an essentially equivalent level of protection to that required under EU law. In assessing whether a country provides an adequate level of protection, the following will be reviewed:

- the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;
- the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Thus the EU/EEA has effectively decided that its own data protection regime is the paradigm example, and what it compares the rest of the world against. Not only does this create an 'us-and-them' mentality but it also has the potential to start a 'data war', and potentially has a discriminatory effect on less economically developed countries which may not have the same resources or same levels of refined governmental,

regulatory or judicial systems. There is also the question as to whether the adequacy decision process will be applied equally to friendly and 'less friendly' nations, or whether it will become the equivalent of international sanctions and be applied on a discriminatory basis in support of geopolitical aims.

Given the UK's compliance with the GDPR to date, and the UK GDPR effectively mirroring the EU GDPR, the UK should, in theory, be deemed to ensure an adequate level of protection and obtain an adequacy decision. However, politics may threaten the UK's chances of an adequacy decision.

On 16 July 2020, the European Court of Justice ("CJEU") invalidated the EU-US Privacy Shield Framework in its decision in the Schrems II case (C-3111/18). The court found that personal data transferred from the EU to the US under the Privacy Shield Framework is not subject to an adequate level of protection i.e. it is not afforded an essentially equivalent level of protection to that required under EU law. In particular, there is an absence of limitation on the powers granted to US government surveillance programmes, and the absence of an effective legal remedy for an EU data subject to challenge how their personal data is processed in that context. This assessment is somewhat ironic given the US Government's position on TikTok. The decision in Schrems II does not mean that transatlantic data transfers can no longer occur, as the CJEU validated Standard Contractual Clauses ("SCC") as a mechanism that ensures appropriate safeguards and compliance with the GDPR. However, if there are any concerns about compliance with SCCs – for example, if the law of a third country overrides contractual provisions – then transfers of personal data under the SCCs will have to cease, as the third country is not providing an adequate level of protection.

The Schrems II decision will form part of domestic case law following Brexit - as with the GDPR, it will be retained EU law – and will have the same precedent and status as existing decisions of the UK Supreme Court. The Supreme Court could choose to depart from Schrems II, or the Secretary of State could take legislative action to depart from the Schrems II decision by making an adequacy regulation in favour of the US. The latter option seems eminently possible given that the UK Government is "disappointed that the EU's adequacy decision for US Privacy Shield has been invalidated". A UK adequacy regulation in favour of the US would mean that the UK was not providing an adequate level of protection i.e. an essentially equivalent level of protection to that required under EU law, and would thus jeopardise the UK's chance of obtaining an adequacy decision. Therefore, whether the UK will obtain an adequacy decision may come down to politics and who the UK wants to align itself with: the US or the EU/EEA. The Internal Market Bill shows the UK Government's readiness to antagonise the EU/EEA, and the UK Government's departure from its previous position and banning the purchase of new 5G equipment from Huawei from January 2021 indicates a leaning for alignment with the US, especially as President Trump takes credit for the UK's change of position. This perceived desire for an alignment with the US may change, however, following the result of the upcoming US Presidential election, and the Internal Market Bill is also causing tensions in the US/UK relationship. The politics of post-Brexit are far from clear, but what is clear is that those politics, whatever they turn out to be, will likely shape the transfer of personal data to the UK and determine whether or not the UK gets an adequacy decision.

Adequacy decisions are not permanent however: they can be repealed, amended or suspended if a third country is no longer ensuring an adequate level of protection. Therefore, even if the UK did obtain an adequacy decision, any future departure from the EU's standard of data protection could result in that adequacy decision being repealed or suspended. Similarly, if other third countries do not follow the EU's rules regarding the transfer of personal data, specifically as regards transfers of personal data to the US in light of the Schrems II decision, then they are arguably not providing adequate protection and so will not obtain an adequacy decision, or their adequacy decision may be suspended/repealed. Thus, data is becoming a commodity to be traded and bartered for, and there is the real risk that the adequacy decision mechanism could become the equivalent of international sanctions and be applied on a discriminatory basis in support of geopolitical aims.

In light of the above, and the very real question as to whether the UK will obtain an adequacy decision, anyone who receives personal data from the EU/EEA should undertake the necessary preparatory work now in order to establish an alternative legal basis for such transfers and ensure the continued flow of personal data from the EU/EEA following Brexit.

UK-Other Third Country Transfers of Personal Data

To ensure that established flows of personal data from the UK to countries and organisations outside the UK and EU/EEA can continue following Brexit, the 2019 Regulations insert provisional arrangements into the DPA 2018. Personal data can continue to be transferred, without further authorisation, from the UK to jurisdictions with a European Commission adequacy decision in place immediately before Brexit, and standard data protection clauses previously issued by the European Commission will continue to be an effective basis for international data transfers from the UK to non-EU/EEA third countries and organisations after Brexit.

As outlined above, going forward, the Secretary of State will be able, through adequacy regulations, to specify that a third country, territory, sector or international organisation (i.e. anything outside the UK) ensures an adequate level of protection of personal data so that transfers of personal data may be made to them without further authorisation.

The considerations as to whether a third country etc. ensures an adequate level of protection of personal data mirror those under the EU GDPR (outlined above). However, after Brexit, the relevant standard when assessing whether a third country etc. affords an adequate level of protection in order to be granted an adequacy regulation will be UK data protection laws rather than EU laws. Thus, the UK will be holding its own data protection regime as the paradigm example, and what it compares the rest of the world against. Again, this creates an 'us-and-them' mentality and potentially has a discriminatory effect on less economically developed countries which may not have the same resources or same levels of refined governmental, regulatory or judicial systems. There are also questions as to whether the adequacy regulation process will be applied equally to friendly and 'less friendly' nations, and whether it will be applied on a discriminatory basis in support of geopolitical aims. For example, in money laundering and tax investigations, the UK has shown clear discrimination against certain countries in its use of account freezing and unexplained wealth orders.

Furthermore, with both the UK and EU/EEA holding out their data protection regimes as the gold standard, if at any point the regimes differ – for example, in relation to the acceptable mechanism for transferring personal data to the US - other countries etc. may be forced into choosing which regime it seeks to comply with in order to facilitate trade, business etc., which could, in turn, have other political consequences.

Data Protection and Litigation under the UK GDPR

It was thought that the introduction of the GDPR would herald the dawn of an unprecedented number data protection breach cases and the imposition eye-watering fines. However, this has not come to pass in either the UK or the rest of Europe. In the UK, although the Information Commissioner's Office (“ICO”) announced its intention to impose fines on British Airways and Marriott in July 2019 (£183.3 million and £99 million respectively), the ICO's negotiations with these companies are still ongoing. Some say that the longer these negotiations continue, the greater the GDPR and its principles are undermined.

The UK’s first fine under the GDPR was in December 2019 against Doorstep Dispensaree Ltd, a pharmacy. The fine was for £275,000, and this was despite its non-cooperation with the ICO’s investigation (a stark contrast with British Airways and Marriott which did cooperate with the ICO) and the ICO’s damning conclusion that the pharmacy's breach “was extremely serious, and demonstrates a cavalier attitude to data protection”. Given this, one might have expected the fine imposed to be higher. However, the Information Commissioner is obliged to ensure that any administrative fines issued in accordance with Article 83 (of both the EU GDPR and the UK GDPR) are effective, proportionate and dissuasive in each individual case and, as the penalty notice states, “The Commissioner has taken into account the size of Doorstep Dispensaree and the financial information that is available about the company on the Companies House website, as well as the representations that Doorsteps Dispensaree has made to her about its financial position."

Thus, the first penalty for breach of the GDPR and the first notices of intent suggest that it will be the financial standing of an individual/company that will ultimately determine the amount of the penalty

imposed. Therefore, large financially-secure corporations, such as British Airways and Marriott, might be likely to pay more heavily for their breaches, even though those breaches may not be as serious as those committed by smaller organisations, and despite their cooperation with the ICO.

The ICO's real focus since the introduction of the GDPR has been reviewing sector/industry-based compliance - ad tech and real time bidding; AI; protection of children's privacy online etc. Some say that the lack of enforcement action by the ICO is because it is not traditionally a prosecuting body and so does not employ many lawyers that specialise in pursuing these types of cases. Therefore, it looks to make deals, and enters into negotiations, despite announcing its intention to impose fines. The outcome of the British Airways and Marriott data breaches and the amount of the fines imposed are likely to indicate how the ICO will pursue enforcement action under the UK GDPR. The COVID-19 pandemic has increased individuals' online presence and increased the amount of personal data that organisations process. This may well provoke the ICO into more severe enforcement action in the event of any breaches of the GDPR (be that the EU GDPR or UK GDPR). However, all the signs to date are that enforcement action will be limited and that there will be room for negotiation.

That said, with the growing realisation that data is a commodity of great value, group actions are being brought in the civil courts to address data protection breaches – for example, the *Morrisons* case ([2017] EWHC 3113 (QB), [2018] EWCA Civ 2339 and [2020] UKSC 12) and *Lloyd v Google* ([2018] EWHC 2599 (QB) and [2019] EWCA Civ 1599). Such group litigation is likely the sign of things to come regarding 'enforcement' under the UK GDPR.

Conclusions

Following Brexit, the UK will have the UK GDPR and, in substance, it will mirror the EU GDPR, both in terms of the obligations it imposes on data controllers and data processors and the rights that it affords data subjects.

However, the one crucial difference, in the rules relating to the transfer of personal data to and from third countries or international organisations, seems likely to be determined by political alliances and has the potential to provide a platform for discrimination in the pursuit of geopolitical aims.

Data has value, especially personal data, and post-Brexit, when its position in the world is looking somewhat uncertain, the UK needs to ensure that it is a place where data can freely and easily flow and be transferred. The UK GDPR and adequacy regulations should not be wielded as a geopolitical tool, but rather as a commercial and business tool, ensuring that the UK's interests are represented, that it is kept international, and ensuring that the UK is continues as a centre for commerce and business.

Ceri Davis

For further guidance, please contact 36 Commercial by calling +44 (0)20 7421 8051 or emailing clerks@36commercial.co.uk