CYBERSECURITY, DATA PRIVACY & INFORMATION MANAGEMENT ALERT

DATA TRANSFERS POST BREXIT

JANUARY 2021

By Barry Fishley and Briony Pollard

2020: a year to remember for myriad of reasons! One being the 'Will we? Won't we have a deal?' nature of the Brexit negotiations. The UK formally left the EU on 31 January 2020 and following an 11 month transition period and months of speculation, the UK's membership of the EU came to an end on 31 December 2020 with an agreement on the future of UK and the EU's relationship. Below we set out what this means for transfers of personal data.

Transfers from the EU/EEA to the UK

One of the key aims of the GDPR is guaranteeing the free flow of personal data inside the European Economic Area ("**EEA**") and prohibiting transfers of personal data to countries outside of it, which are not considered to provide an adequate level of data protection, unless an exception or additional safeguard is in place. Up until the end of the transition period, the UK was in the EEA and accordingly, personal data could be transferred between the UK and the EEA and vice versa without additional safeguards being in place. Now that the UK has left the EU, for data protection purposes, the UK is considered a 'third country' within the meaning of the GDPR. This means that transfers of personal data from the EEA to the UK can only take place if (i) the UK is determined by the EU to offer an 'adequate' level of protection to personal data; (ii) a derogation for occasional and non-repetitive transfers applies e.g. consent; or (iii) additional safeguards are in put in place e.g. EU model standard contractual clauses ("**SCCs**") or binding corporate rules ("**BCRs**").

The European Commission ("**EC**") has the power to determine whether a country outside the EEA offers an adequate level of data protection by adopting an adequacy decision. When a decision has been adopted, this means that data can be transferred without any additional safeguards. The EC is yet to make an adequacy decision in favour of the UK, indeed the assessment is ongoing, which means that in the absence of a derogation e.g. consent or performance of a contract, the entity transferring personal data to the UK must ensure that an additional safeguard is in place e.g. SCCs or BCRs between the transferring and receiving entities.

The EU-UK Trade and Cooperation Agreement i.e. the 'deal' between the UK and the EU, includes a 'bridging mechanism' i.e. an interim solution, which allows organisations that transfer personal data from the EEA to the UK, to continue to do so, for a grace period, to give time for the EC to determine whether an adequacy decision can be made in favour of the UK. During the grace period, transfers of personal data from the EEA to the UK will not be considered transfers to a 'third country'. The grace period is for an initial four months, but may be extended by two months unless the UK or EU objects. If the UK amends its data protection legislation, or exercises certain designated powers without EU agreement during the grace period, the grace period will end.

The granting of an adequacy decision by the EC at the end of the grace period is not guaranteed. In the event an adequacy decision is not determined, transfers of personal data from the EEA to the UK will require an additional safeguard (e.g. SCCs or BCRs) to be in place between the transferring and receiving entities.

Transfers from UK to EEA

The UK Government determined that a transitional adequacy decision is in place to cover transfers of personal data from the UK to the EEA. This means, that for the mean time, there is no change to the pre-Brexit position. Transfers can continue to be made without any additional steps being taken or documents put in place. Transfers to Gibraltar will also continue to be permitted.

Transfers of personal data from the UK to countries other than the EEA i.e. rest of world ('**ROW**')

If an entity is transferring personal data from the UK to a ROW country, it should already have a GDPR compliant mechanism in place to allow for such transfer e.g. an adequacy decision (albeit made by the EC), reliance on a derogation e.g. consent or additional safeguard e.g. SCCs, BCRs. Post-Brexit, the UK government has confirmed that UK organisations may continue to rely on the same mechanisms.

Where an organisation has had their BCRs approved by a European regulatory authority, it is automatically eligible for UK BCRs. The only step required is for the entity to notify the UK data regulatory authority, the Information Commissioner's Office, of the fact that the entity holds EU BCRs and wishes to hold UK BCRs.

Note that if an organisation is using BCRs or SCCs for such transfers, following the CJEU decision in *Schrems II*, the transferring entity is required to conduct a risk assessment to ensure that the SCCs provide an 'essentially equivalent' level of protection

CYBERSECURITY, DATA PRIVACY & INFORMATION MANAGEMENT ALERT
DATA TRANSFERS POST BREXIT

JANUARY 2021

to that under the GDPR, which may involve putting in place 'supplementary measures' in addition to the BCRs or SCCs. The consultation on the European Data Protection Board's ("**EDPB**") draft recommendations on the supplementary measures that should be put in place alongside the SCCs ended on 21 December 2020. Once the EDPB publishes its final recommendations, the UK data supervisory authority, the Information Commissioner's Office, intends to publish its own guidance on the topic so we recommend keeping an eye out for that.

We also await the updated drafts of the SCCs from the EC. The EC's consultation on its draft SCCs ended on 10 December 2020 and whilst there have been no further developments from the EC itself, the EDPB and European Data Protection Supervisor have published a joint opinion (as requested by the EC) on the draft SCCs. The opinion invites the EC to clarify a number of issues in the revised SCCs, including whether the modules for different transfer scenarios (i.e. controller-controller, controller-processor, processor-processor and processor-controller) can be applied in one set of SCCs between parties, through additional guidance such as flowcharts and FAQs. Once adopted organisations will have twelve months to use the new SCCs.

Transfers of personal data from non-EEA country to UK

Again, there is no change to the pre-Brexit position. It is the responsibility of the transferring entity to ensure they are complying with the data transfer rules that apply in their jurisdiction when they transfer personal data to the UK. Upon receiving the data, the receiving entity still needs to comply with the data protection rules in the UK, as was the case, pre-Brexit.

Key takeaways

- We recommend that organisations review and update their privacy policies and notices, both internal and external, to reflect the revised position in relation to international transfers of data.
- In order to be on the front foot in the event that the EC does not grant an adequacy decision in respect of the UK by the end of the grace period, we recommend that organisations review their relationships with third parties and consider whether agreements with them will need to be updated with SCCs, to ensure data is being transferred to them and back to the organisation legally, so that they may put such additional safeguards in place in short order, if necessary.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
Briony Pollard	View Bio	briony.pollard@weil.com	+44 20 7903 1372