SLAUGHTER AND MAY/

CLIENT BRIEFING

NOVEMBER 2020

INTERNATIONAL TRANSFERS OF PERSONAL DATA

A WAY FORWARD?

The CJEU Schrems II decision in July caused consternation in relation to international transfers of personal data out of the EEA and, initially at least, raised more questions than it answered. However, a number of these have now been answered following publications by the European Data Protection Board ('EDPB'). In addition, the European Commission has recently published a draft of the updated standard contractual clauses for transferring personal data to non-EEA countries ('SCCs'). This briefing therefore considers what organisations should do now.

Data mapping

As acknowledged by the EDPB in its draft Recommendations 1/2020 ('EDPB Recommendations'), data mapping is the first step and one which all organisations transferring personal data out of the EEA should undertake. The EDPB recognises the complexity of recording and mapping all data transfers but it still requires a detailed approach, taking account of onward transfers, data minimisation requirements and identifying where cloud services are used. Many organisations have data mapping processes built into their compliance programmes given the GDPR's requirements around records of processing and transparency, and so these may already be sufficient, or at least a good starting point.

Transfers currently relying on an adequacy decision or derogation

If an adequacy decision is in place for a non-EEA country, no further assessment or steps are required for the transfer to proceed. In addition, although the EDPB reminds us that derogations (e.g. explicit consent or performance of a contract) are narrow and only for occasional transfers, it would seem that if one is applicable, the EDPB considers any further assessment to be equally unnecessary.

Transfers currently relying on SCCs

The EDPB Recommendations set out a step-by-step approach for data exporters to help them determine whether their transfers of personal data to outside the EEA may proceed in compliance with EU law. The aim here is to verify, prior to any transfer, that the level of protection for personal data in the recipient country is 'essentially equivalent' to the level of protection under EU law.

For transfers that rely on SCCs (or any other transfer tool other than adequacy or derogations), the remaining steps include:

- assessing the laws or practices of the recipient country;
- adopting any necessary supplementary measures;
- taking any formal procedural steps required by the supplementary measures; and
- regularly reviewing the level of protection in the recipient countries to which the data is transferred.

How to assess the laws of a third country

The EDPB states that data exporters must assess, where appropriate in collaboration with the importer, if there is anything in the law or practice of the third country that may impinge on the effectiveness of the transfer tool relied on, in the context of each specific transfer. This means assessing and documenting the specific circumstances of the transfer (e.g. entities involved, purpose, sector of recipient, type of access etc), but also, more importantly, assessing the laws and practices of the third country. Those relating to access by public authorities to personal data for surveillance purposes will be particularly, though not solely, relevant. This is an area which is likely to cause some concern and difficulties for organisations, given how opaque surveillance measures can be in some countries.

The EDPB does provide some guidance on how to assess surveillance measures in its Recommendations 2/2020 on the European Essential Guarantees for surveillance measures (adopted on 10 November), with interference with data privacy rights by surveillance measures only being justifiable where certain essential guarantees are in place.

Transfers to the US

According to the CJEU and the EDPB, the surveillance measures in the US (in particular Section 702 FISA and Executive Order 12 333) are neither sufficiently limited nor provide for effective redress for individuals to enforce their rights, as required under EU law. It will therefore be particularly important to ensure robust supplementary measures are in place, although this may still not always be sufficient depending on the transfer in question.

The EDPB and the EU Commission have adopted slightly different approaches on the question of whether an organisation can take account of the likelihood of public authorities accessing the data. Hopefully, this will be clarified in the final versions.

What are supplementary measures?

Supplementary measures 'fill in the gaps' where the laws of a third country together with the use of appropriate safeguards do not meet the required level. The EDPB's draft supplementary measures will come as no surprise to those that have been monitoring and commenting on the topic of international transfers since July, as they cover, amongst other things, encryption, data mnimisation and contractual reporting of surveillance requests.

Helpfully, case studies are included showing how the supplementary measures could be applied. However, in some situations the EDPB states that it cannot contemplate any additional safeguards being sufficient (e.g. cloud services in the US where there is access to the data or intragroup transfer of HR data to a US parent).

The draft Recommendations are available for public consultation until 30 November 2020 and will be applicable immediately following their publication in final form.

Updated SCCs

The EU Commission has published drafts of the udpated SCCs. Helpfully, these cover the full range of the transfer scenarios that organisations might need, including processor to controller and processor to sub-processor. The consultation ends on 10 December. Whilst the EU Commission had relatively recently talked about the new SCCs being in place by the end of 2020, this is now looking somewhat optimistic.

There is grandfathering of the existing SCCs for a maximum of one year (sooner if the underlying agreement is amended other than to include safeguards or supplementary measures per Schrems II). The new SCCs will therefore need to be entered into within this period unless the relevant processing terminates by the deadline.

Conclusion

Many organisations had sensibly chosen to adopt a 'wait and see' approach in the immediate aftermath of Schrems II. Whilst it may be possible to justify this approach until the EDPB Recommendations are in final form, it is clear that time is fast running out. Organisations would therefore be well advised to start planning, if they haven't already, for this new regime with its attendant resourcing implications.

CONTACT

REBECCA COUSIN
PARTNER, CO-HEAD OF DATA PRIVACY
T: +44 (0)20 7090 3049
E: rebecca.cousin@slaughterandmay.com

CINDY KNOTT
DATA PRIVACY PROFESSIONAL SUPPORT LAWYER
T: +44 (0)20 7090 5168
E: cindy.knott@slaughterandmay.com