WALKERS

Global Legal and Professional Services

Ireland Update – Data Privacy – International Data Transfers

December 2020

Introduction

In our October 2020 advisory, we highlighted the uncertainty in respect of data transfers between the EU and UK from the end of the Brexit transition period on 31 December 2020 (the "**Transition End Date**").

Against this backdrop, there have been a number of developments in recent weeks with regard to the obligations of EU-based organisations transferring data to third countries. These developments include the publication of new draft measures from the European Data Protection Board (the "**EDPB**") and the EU Commission which should be considered in tandem and are detailed below.

Background

The Court of Justice of the European Union (the "**CJEU**"), in its July "Schrems II" decision, struck down the US Privacy Shield mechanism and found that the European Commission's standard contractual clauses ("**SCCs**"), in their current form, continue to be a valid mechanism for the transmission of personal data outside the EEA. SCCs seek to contractually ensure an 'essentially equivalent' level of protection for data transferred to third countries.

However, transferring parties using SCCs to transfer personal data to a third country must now carry out an assessment, prior to making data transfers under SCCs, as to whether the law of the third country to which the data is being transferred impinges on the effectiveness of the safeguards provided by the SCCs.

On the basis of the outcome of that assessment, organisations using SCCs to govern transfers of personal data to third countries may now need to take additional steps to ensure the protection of the data they are transferring (e.g. by implementing "supplementary measures").

The EDPB Recommendations

Since the delivery of the "Schrems II" judgment, there has been no guidance available to transferring parties to assist in determining which supplementary measures should be introduced.

The EDPB has now adopted draft recommendations, which are the subject of a public consultation, in respect of the use of the transfer mechanisms for data transfers to third countries (the "**EDPB Recommendations**"). The EDPB Recommendations will assist data exporters in assessing their practices in relation to data transfers to a third country, in particular, determining whether supplementary measures are required in addition to SCCs and, if so, which supplementary measures would be most appropriate.

The EDPB Recommendations set out 6 steps that data exporters should take in assessing their data transfers to third countries:

1. Map all existing data transfers to third countries.
2. Identify the transfer mechanism the data transfer relies upon (e.g. SCCs).
3. Assess the laws or practice of the third country to which data is being transferred that may impinge on the effectiveness of the safeguards provided by the transfer mechanism being relied upon.
4. Identify and adopt supplementary measures as appropriate.
5. Take any formal procedural steps the adoption of your supplementary measure may require.
6. Re-evaluate steps taken in light of any further developments.

The EDPB Recommendations recognise that controllers or processors, acting as data exporters, are responsible for verifying, in collaboration with the data importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the transfer mechanisms for data transfers to third countries.

The supplementary measures suggested for use by the EDPB Recommendations include technical measures, additional contractual measures and organisational measures. The EDPB Recommendations make clear that the supplementary measures that provide the greatest degree of protection for personal data transferred to third countries are technical measures, most particularly, secure encryption and pseudonymisation of personal data. Organisational measures such as internal policies, organisational methods and standards may serve to complement contractual and/or technical measures.

The SCC Implementing Decision

The European Commission has published a draft implementing decision on SCCs for the transfer of personal data to third countries which includes an annex setting out the text of the updated SCCs, which is also the subject of a public consultation (the "SCC Implementing Decision").

At present, SCCs are one of the most widely used transfer mechanisms for transfers of personal data from within the EU to third countries. SCCs may be put in place either as a standalone agreement or by incorporating the SCCs into existing agreements. Under the SCC Implementing Decision, data exporters will need to phase out and replace all existing SCCs within 12 months of the adoption of the SCC Implementing Decision. The annex to the SCC Implementing Decision sets out the text of the updated SCCs and categorises them as follows:

- Controller-to-controller transfers;
- Controller-to-processor transfers;
- Processor-to-processor transfers; and
- Processor-to-controller transfers.

The latter two are new categories for which SCCs were not previously provided and will provide legal certainty in processor-to-sub-processor transfers which are quite common.

The SCC Implementing Decision cross-refers to the EDPB Recommendations and proposes to implement some of the supplementary measures. Examples of supplementary contractual measures include the insertion of a requirement that the data importer should, to the extent possible, notify the data exporter and the data subject if it receives a legally binding request to disclose personal data by a public authority under the law of the country of destination or becomes aware of any direct access by public authorities to personal data transferred pursuant to the SCCs in accordance with the law of the third country of destination.

Where it is not possible to ensure the protection of personal data transferred to a third country, including by means of a supplementary measure, the CJEU suggests that those transfers should be suspended.

Next steps

Data exporters should:

» Carry out a mapping exercise of any all third country data transfers.

» Identify the third country data transfer mechanism most suitable to their needs.

» Carry out an assessment to verify, prior to any transfer, whether the level of protection of personal data in the third country to which personal data is being transferred is 'essentially equivalent' to the level of protection in the EU.

» Carry out a risk analysis of personal data being transferred and consider underlying risks in determining what additional supplementary measures might be appropriate.

» Identify and adopt suitable supplementary measures based on the results of this assessment.

How can Walkers help?

The Walkers Data Privacy Team are ready to assist clients by advising on the steps required to ensure ongoing compliance of international data transfers.

Key Contacts

If you would like to discuss any of the issues dealt with in this advisory, please contact the below or your usual Walkers contact.

Eoin O'Connor
Partner
T: +353 1 470 6664
E: eoin.oconnor@walkersglobal.com

Shane Martin
Of Counsel
T: +353 1 470 6673
E: shane.martin@walkersglobal.com

Conor Daly
Senior Associate
T: +353 1 470 6684
E: conor.daly@walkersglobal.com