KIRKLAND & ELLIS

Kirkland Alert

Demystifying *Schrems II*: EU Commission and European Privacy Watchdog Publish Instructive Guidance and Recommendations

21 December 2020

Four months on from the seminal Court of Justice of the European Union ("CJEU") decision in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* (Case C-311/18) ("*Schrems II*"), eagerly anticipated guidance has been released by both the European Commission and the European Data Protection Board (the "EDPB") with the objective of helping businesses comply with the enhanced obligations introduced by *Schrems II* in relation to the transfer of personal data outside the European Economic Area (the "EEA").

These publications include:

- The EDPB guidance on supplementary transfer tools to ensure compliance with the EU level of protection of personal data (the "Supplementary Measures Guidance");
- The EDPB guidance on essential guarantees for surveillance measures (the "Surveillance Recommendations"); and
- The European Commission's draft implementing decision which contains new draft Standard Contractual Clauses for use in various data transferring contexts (the "New SCCs").

The Supplementary Measures Guidance is open for public consultation until 21 December 2020 while the Surveillance Recommendations were adopted outright. The consultation period for the New SCCs closed on 10 December and the New SCCs are expected to be adopted in early 2021.

This *Kirkland Alert* summarises, at a high level, the key points from the guidance and contractual terms published by the EDPB and the European Commission and sets out some tips for the practical implementation of these recommendations for businesses

that transfer, or are looking to transfer, personal data from the EEA to the US (and to other third countries).

The Current State of Play Following the *Schrems II* Decision

As reported by us here, in July 2020, the CJEU delivered a judgment which significantly impacted the legal framework for legitimising international transfers of personal data to countries based outside the EEA ("third countries"). At a very high level, CJEU determined in *Schrems II* that:

- the EU-US Privacy Shield is not an acceptable basis to legitimise transfers from the EU to the US and is therefore invalid; and
- the European Commission's Standard Contractual Clauses (the "SCCs") remain valid as a data transferring mechanism *subject to the adoption of supplementary measure*s.

As a result of the *Schrems II* decision, in respect of continued reliance on SCCs, data exporters are now under an obligation to assess, analyse and verify on a case-by-case basis that the personal data being transferred will be adequately protected in the country to which the personal data is being exported, in line with the requirements of EU law. In particular the data exporter should consider if the relevant public authorities in the third country may have legal rights of access to the personal data and what mechanisms exist to limit such access.

The CJEU did not outline what specific supplementary measures should be adopted to legitimise transfers, or the criteria for assessing whether the laws of a third country ensure an adequate level of protection. Accordingly, data exporters seeking to rely on SCCs in the aftermath of *Schrems II* were left in a state of uncertainty as to what appropriate remediation steps ought to be adopted.

The EDPB guidance and the new draft SCCs have therefore provided businesses with much anticipated and welcome guidance on how to facilitate the uninterrupted flow of personal data to countries outside the EEA in the wake of *Schrems II*.

EDPB Guidance on Supplementary Measures (Supplementary Measures Guidance)

The Supplementary Measures Guidance assists data exporters in identifying suitable technical safeguards that can be applied, and appropriate contractual terms that can be implemented, to protect personal data being transferred to third countries outside the EEA ("Third Countries"). In particular, a roadmap of six practice steps is set out to assist data exporters in bringing data transferring mechanisms in line with the standard prescribed by the CJEU in *Schrems II*.

1. **Data Transfer Mapping**: All transfers of personal data to Third Countries should be documented. The Supplementary Measures Guidance suggests updating and expanding existing records of processing activity inventories to document this information.
2. **Identify Transfer Tool**: Data exporters should, in the case of each transfer of personal data to a Third Country, identify which mechanism is being relied on to legitimise the transfer (e.g., the SCCs, Binding Corporate Rules, or a derogation as set out in Article 49 of the GDPR, such as data subject consent). As reported by us here, following *Schrems II* the EU-US Privacy Shield is no longer a valid mechanism for legitimising transfers of personal data from the EU to the US.
3. **Assess Effectiveness**: In relation to each specific transfer to a Third Country *not* based on an 'adequacy decision' (i.e., a finding by the European Commission that the laws of that country provide an adequate level of protection for personal data (a full list of such countries is available here) data exporters are now required, in collaboration with the relevant data importers, to conduct a documented due diligence exercise to assess whether any local law provisions may impinge on the effectiveness of the appropriate safeguard being relied on.
4. **Adopt Supplementary Measures**: Where the assessment carried out under Step Three identifies deficiencies in the laws of a Third Country, data exporters are required to adopt supplementary measures to ensure that a level of protection is applied to the transfer that is equivalent to that available to protect personal data under EU laws. Annex 2 of the Supplementary Measures Guidance further details a non-exhaustive list of examples which can be applied (summarised below). These can be technical, contractual or organisational in nature.
5. **Procedural Steps**: Data exporters may need to take certain formal procedural steps to adopt any required supplementary measures which may include consulting with and/or obtaining authorisation from, a competent supervisory authority.
6. **Re-evaluate**: On completing steps one to five, data exporters should put in place a framework to facilitate ongoing compliance with these enhanced obligations. This framework, together with the measures adopted, and the assessment of Third County laws, should be continuously monitored and, if necessary, updated

to reflect any developments affecting the level of protection afforded to the personal data.

As discussed above, Annex 2 of the Supplementary Measures Guidance sets out a non-exhaustive list of supplementary measures which can be adopted by data exporters and which may, depending on the context and characteristics of the transfer, ensure the required level of protection. Such measures include:

- **Technical Measures**: The EDPB emphasises that any encryption algorithms adopted to help secure data transfers should conform to the state of the art and should be implemented by properly maintained software. In addition, encryption keys should be reliably managed and controlled by the data exporter. Any additional information which can be used to re-identify pseudonymised data should be held exclusively by the data exporter.
- **Contractual Commitments**: Data importers should be placed under obligations to assist with any assessment of Third Country data privacy laws. In addition, the EDPB recommends that contractual terms between data exporters and importers contain extensive audit rights in favour of the exporter (to evaluate compliance with the SCCs by the importer), and obligations on the data importer to notify the data exporter in the event it is unable to comply with contractual commitments.
- **Organisational Measures**: Certain organisational measures can be implemented by data importers to enhance the standard of protection for personal data. These include, data security certification, the implementation of comprehensive data protection notices, regular review of internal policies, and effective staff training.

EDPB Recommendation on Surveillance Measures (the Surveillance Recommendations)

The Surveillance Recommendations supplement the European Essential Guarantees Guidance adopted by the Article 29 Working Party in 2016 and are intended to assist data exporters and importers in assessing when the surveillance laws of a Third Country which interfere with individual privacy rights constitute a warranted interference or, when any such laws mandate the invalidation of the transfer.

The Surveillance Recommendations establish four "European Essential Guarantees" (the "EEGs"), which can be summarised as follows:

- **Guarantee A (Clear Rules)**: Processing should be based on clear, precise and accessible rules. Any Third Country surveillance laws should be clearly

communicated to data subjects and include information regarding the individuals who may be subject to the surveillance.

- **Guarantee B (Necessity & Proportionality)**: Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated. The EDPB specifies that the principle of necessity mandates that Third Country surveillance laws should not authorise public authorities to access personal data on a generalised basis. In relation to the principle of proportionality, this requires: (1) an assessment of the severity of any interference by surveillance laws with individual rights, and (2) a verification of the public interest objective pursued.
- **Guarantee C (Independent Oversight)**: The EDPB specifies that an effective and impartial system should oversee any interference with privacy rights.
- **Guarantee D (Effective Remedies)**: Effective remedies and redress need to be available to the individual. The key criteria in determining whether a decision making body offers sufficient redress include: independence, adopted rules of procedure, powers to remedy non-compliance, and no evidential barriers to filing an application.

The EEGs are likely to serve as a useful reference point for data exporters and importers when conducting due diligence on the surveillance laws of Third Countries as recommended by step three of the Supplementary Measures Guidance.

New Standard Contractual Clauses

In November 2020, the European Commission published a draft implementing decision to which the New SCCs are annexed.

The New SCCs adopt a modular format and accommodate four different personal data transferring scenarios, namely: (1) Controller-to-Controller ("C2C"), (2) Controller-to-Processor ("C2P"), (3) Processor-to-Processor ("P2P"), and (4) Processor-to-Controller ("P2C").

While C2C and C2P personal data transferring relationships were addressed under the existing SCCs, they have now been updated to reflect the complexity of modern data processing activities. In relation to P2P and P2C relationships, the EU Commission has for the first time facilitated active compliance by processors as data exporters. This is a more flexible and pragmatic approach, which ultimately reflects the view of the CJEU in *Schrems II* that it is the shared responsibility of both the data importer and exporter to ensure that adequate safeguards are applied to international transfers of personal data.

The New SCCs also contain specific safeguards to assist data exporters and importers to comply with the obligations mandated by the *Schrems II* decision, for example, an obligation to question and, where appropriate, challenge any governmental data access requests.

The New SCCs were published in draft form and were open for public consultation which closed on 10 December 2020. It is anticipated that the New SCCs will be formally adopted in early 2021 and will replace the current SCCs.

Data exporters and importers that rely on the current SCCs as a data transferring mechanism may continue to do so (unless there are material changes to the contract) and will have a one-year grace period to implement the New SCCs. This grace period will commence on the date that the New SCCs are formally adopted by the EU Commission (expected to be early 2021).

Next Steps for Businesses

This regulatory guidance provides welcome clarity to businesses seeking to address any vulnerabilities in their data transfer arrangements, which have been brought into focus by the *Schrems II* decision. We have set out below some key points and practical compliance tips for businesses as they now, in light of these developments, seek to move forward with a formalised compliance programme.

- In the event that the UK does not receive a finding of adequacy from the EU Commission before the expiry of the Brexit transition period (31 December 2020), it should be treated as a "third country" for the purposes of the GDPR until such time as an adequacy decision is forthcoming.
- Businesses exporting personal data to the US or to other Third Countries outside the EEA (which, as noted above, could shortly include the UK) may now wish to undertake a remediation project to analyse their data transfer arrangements as outlined in **steps one to three** of the Supplementary Measures Guidance (summarised above).
- Where any such transfers are based on SCCs (in their current form), these will need to be replaced with the New SCCs (once formally approved and adopted). Businesses will have a one-year grace period to complete this exercise from the formal adoption of the New SCCs (likely to be in early 2021).
- Reliance by businesses on any of the 'appropriate safeguards' set out in Article 46 of the GDPR (whether Binding Corporate Rules, SCCs or an approved code of conduct) will always require businesses to complete the assessment and remediation

exercises described in steps **four to six** of the Supplementary Measures Guidance roadmap (summarised above).

- Businesses transferring personal data to countries that have been deemed adequate by the European Commission, do *not* need to take any further steps once this information has been charted and documented, however, a framework should be put in place to continuously monitor that any such EU Commission adequacy decision(s) remains valid and in effect.
- All businesses transferring personal data outside the EEA should now update their GDPR compliance frameworks to ensure: (1) continued evaluation of Third Country surveillance laws, (2) the implementation of robust technical and organisational measures to protect any personal data transferred; and (3) effective staff training on these enhanced requirements along with the consequences of non-compliance for your business.

Authors

Emma L. Flett

Partner / London

Jennifer F. Wilson

Partner / London

Anna Ní Uiginn

Associate / London

Related Services

Practices

- Intellectual Property
- Technology & IP Transactions

Suggested Reading

- 10 August 2020 Kirkland Alert *Schrems* Strikes Again: EU-US Privacy Shield Suffers Same Fate as its Predecessor

- 05 May 2020 Kirkland Alert California Court of Appeal Clarifies Standard for Reasonable Royalty Determination Under California's Uniform Trade Secrets Act
- 16 April 2020 Kirkland Alert NAD Launches New Fast-Track SWIFT Challenge Process to Expedite Time-to-Decision for Well-Defined Single-Issue Cases