International Data Transfers | Privacy

The new SCCs December 2022 deadline is approaching, are you prepared?

Schrems II has significant implications for your organisation if you transfer personal data outside of the **EEA**. The **deadline** to identify, assess and remediate all existing contracts with the new Standard Contractual Clauses ("new SCCs") **is 27 December 2022**.

27 December 2022

What happened?

Schrems

The Schrems II Case led to the invalidation by the Court of Justice of the European Union (CJEU) of the Privacy Shield as a data transfer mechanism between the EU and the US. The invalidation of the EU-US Privacy Shield in July 2020 meant that **all transfers relying on the Privacy Shield had to immediately cease.** The case also scrutinised the effectiveness of the SCCs.

The CJEU decision on SCCs

The CJEU advised that organisations must, on a case by case basis, verify that the personal data of EU citizens being transferred outside of the EEA will be adequately protected in the third country in line with the level of protection set out in the GDPR, taking into account local law and government practices. This assessment of transfers is conducted via Transfer Impact Assessments (TIA).

New SCCs

SCCs are one of the key mechanisms to legally transfer personal data from the EEA to third countries which do not benefit from an EU adequacy decision. However, as a result of the judgement the SCCs had to be redrafted. Old SCCs, those that were adopted under the previous Data Protection Directive 95/46, can no longer be used.

Guidance

European Commission guidance in relation to new Standard Contractual Clauses

The European Commission released updated SCCs. The new SCCs aim to extend the protection of personal data set out in the GDPR to third countries who process the personal data of EU citizens, and who have not secured an Adequacy Decision from the European Commission.

European Data Protection Board Recommendations on Measures that Supplement Transfer Tools

The EDPB released Recommendations to support organisations with their obligation to identify and implement appropriate supplementary measures, where the transfer tool selected does not provide an equivalent level of protection offered under the GDPR.

Supplementary Measures should be used with the existing data transfer tool, such as SCCs. Examples of Supplementary Measures include:

- Technical measures;
- Organisational measures; and
- Additional contractual measures.

European Commission FAQs

In May 2022, The European Commission published guidance outlining questions and answers on the new SCCs. The Q&A offers practical guidance on the use of SCCs and assists stakeholders in compliance efforts.

European Data Protection Board Guidance

The EDPB Guidance provides a step-by-step roadmap to identify if organisations exporting data are required supplementary measures in place to ensure personal data is being transferred legally outside the EEA. The Guidance outlines the steps involved for assessing and protecting cross border personal data flows in line with EU law.

See below the roadmap as recommended by the EDPB.

The 6 Steps as recommended by the EDPB:

Step 1
Know your transfers

An organisation must understand the flow of their personal data and identify in-scope contracts to "ensure that it is afforded an essentially equivalent level of protection wherever it is processed."

Step 2
Identify your transfer tools

The Commission has stated that the U.S. is not recognised as providing "adequate" protection. Therefore organisations must rely on transfer tools outlined in Article 46 of the GDPR for transfers to third countries.

Step 3
Assess the sufficiency of non-EEA protections

An organisation is expected to assess the third country to which the personal data is transferred. The organisation must then decide if supplementary measures are required to protect the data.

Step 4
Identify and Adopt supplementary measures

The Guidelines outline factors to consider in identifying appropriate supplementary measures and a 'non-exhaustive' list of supplementary measures that can be implemented.

Step 5
Take Formal Procedure steps

An organisation is expected to take the relevant procedural steps to remediate the in-scope contracts and adopt any supplementary measures identified to protect personal data.

Step 6
Re-evaluate periodically

An organisation is advised to re-evaluate the data transfer at appropriate intervals and monitor any developments which may affect the transfer of personal data to the third country.

Latest Guidance: FAQs issued by the European Commission

In May 2022, the European Commission issued FAQs on the new SCCs . Some key messages include:

- The SCCs cannot be used to transfer data to non-EEA importers who are already subject to the GDPR;
- Electronically executed contracts are only permitted where also permitted under national contract law;
- Modifications to SCCs are restricted to listed scenarios within the FAQs;
- Only the Modules that are applicable should be used. This means that the Modules that are not applicable should be removed from the contract; and
- Notification of the obligations of Data Importers regarding access of Public Authorities are clarified.

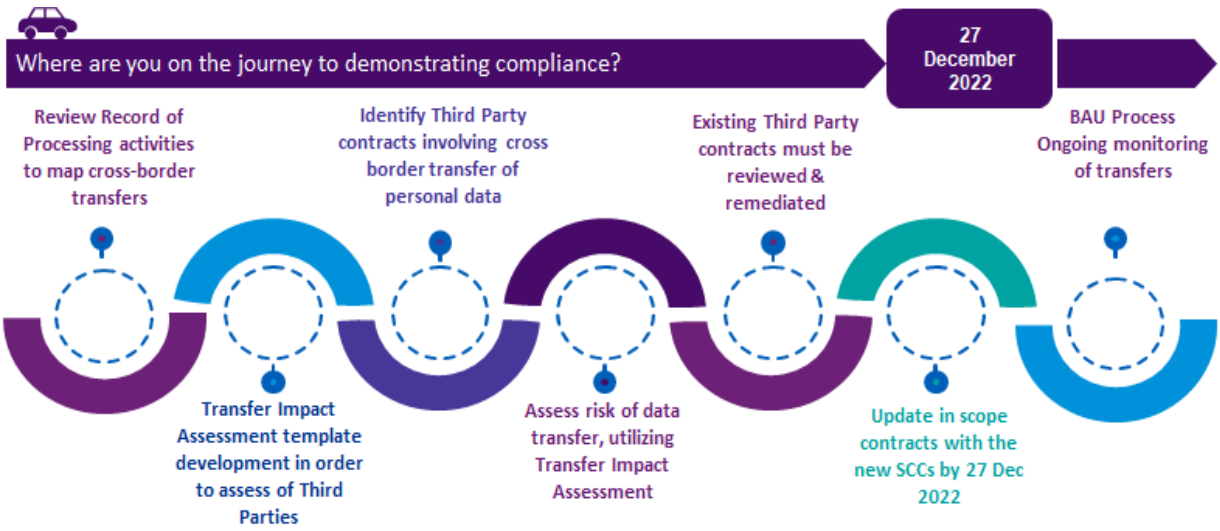
New UK Standard Contractual Clauses UK GDPR

In February 2022, the United Kingdom introduced **a draft international data transfer agreement** ("IDTA") and **an additional addendum** to the European Commission's 2021 standard contractual clauses for international data transfers ("**UK Addendum**"). The documents came into force on **21 March 2022.**

This means that organisations transferring **personal data from the UK** to third countries outside the EEA must also examine their data flows and may be required to update their existing transfer mechanisms.

If organisations have already entered into the EU's pre-GDPR SCCs, organisations may continue to use them until March 2024.

Key steps to consider



As your organisation navigates this challenging landscape, KPMG can help you prepare for the steps you need to take.

Contact Us

Michael Daughton
Partner
Risk and Regulatory Consulting
t: +353 87 744 2965
e: michael.daughton@kpmg.ie

Tom Hyland
Director
Privacy - Risk and Regulatory Consulting
t: +353 87 050 4223
e: tom.hyland@kpmg.ie

Fiona Bresnihan
Associate Director
Privacy - Risk and Regulatory Consulting
t: +353 87 111 6963
e: fiona.m.bresnihan@kpmg.ie

Daniela Mejuto Pita
Manager
Privacy - Risk and Regulatory Consulting
t: +353 86 137 1123
e: daniela.mejuto-pita@kpmg.ie