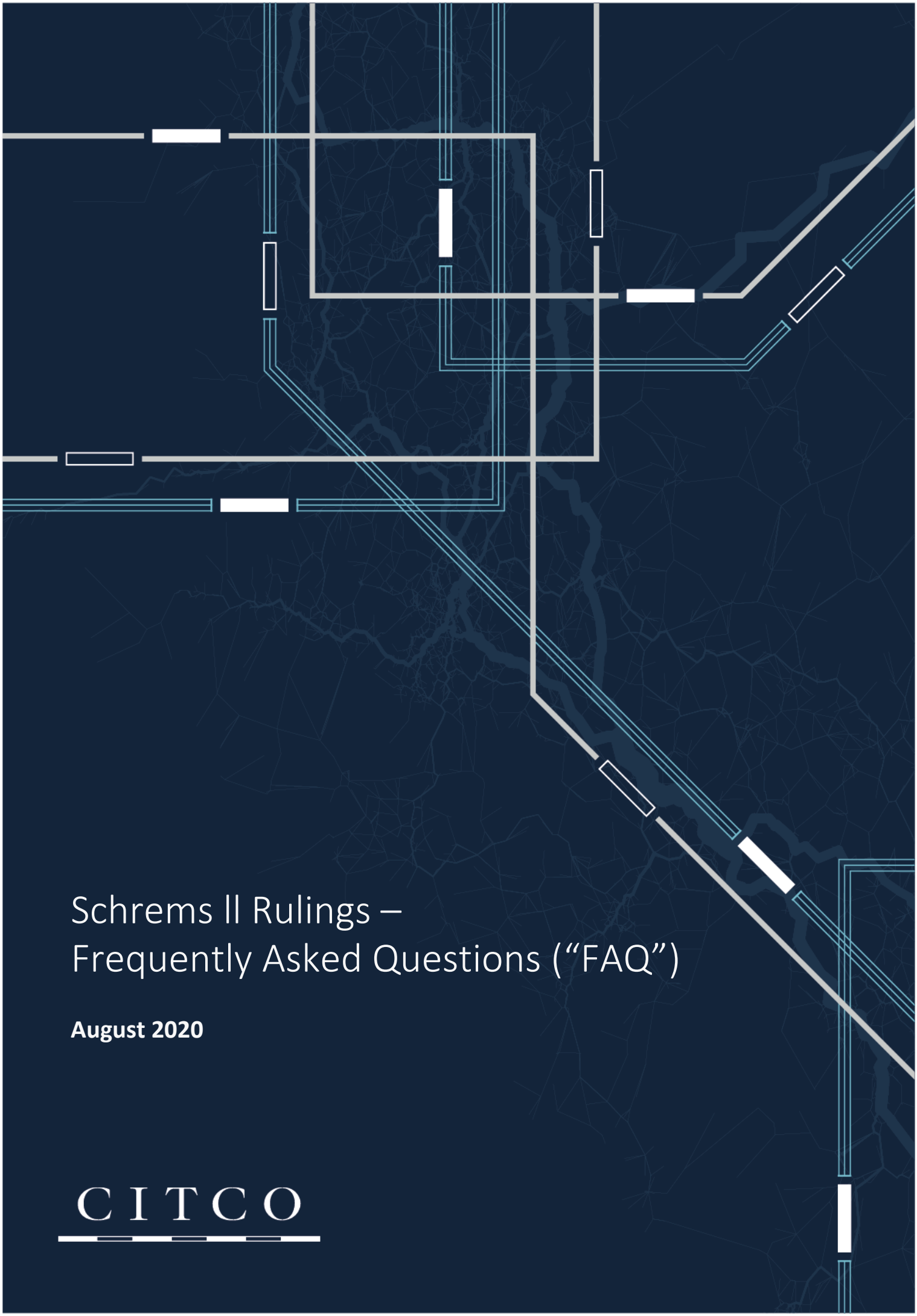

Schrems II Rulings – Frequently Asked Questions ("FAQ")

August 2020

CITCO

The following questions and answers are provided as general information regarding the Court of Justice of the European Union (CJEU) ruling C-311/18 (commonly referred to as the "Schrems II" ruling) and will be updated from time to time and/or upon the release of European Commission, European Data Protection Board and supervisory authority guidelines and practice directions which are expected to be published in the near future. The information contained herein should not be construed as legal opinion or advice on any subject matter.

1. What was the CJEU Schrems II ruling?

Data Protection Commissioner –v- Facebook Ireland Limited and Maximillian Schrems (Schrems II) C-311/18

On 16 July 2020, the CJEU declared the Privacy Shield (a legal mechanism that allows the lawful transfer of personal data from the European Economic Area (EEA) to the United States of America (US)) invalid with immediate effect on the basis that it does not provide *"essentially equivalent"* protection of personal data.

In the same ruling, the CJEU upheld but qualified the use of Standard Contractual Clauses (SCCs) (another mechanism allowing lawful transfers from the EEA to the US) as not being enough for certain EEA to US personal data transfers arrangements to take place.

2. What Citco group of companies ("Citco") entities are impacted by the ruling?

The findings of the Schrems II ruling concern data transfers from the EEA to the US and other third countries and it impacts organisations (exporting personal data) that are within the scope of the GDPR. Organisations not within the scope of the GDPR[1] that transfer personal data to US and other third countries are not impacted by the findings of the case.

Many of Citco's service entities are outside the territorial scope of the GDPR and so are not impacted by the Schrems II ruling. Citco entities that are within the scope of the GDPR (and the Schrems II ruling) are hereinafter referred to as "in-scope Citco entities".

1 i.e. Within the scope of the GDPR by reason of (i) GDPR Article 3(1) established in the EEA; or (ii) GDPR Article 3(2) offering of goods/services to individuals in EEA or monitoring the behaviour of such individuals.

3. What are the implications for Citco now that the EU-US Privacy Shield is invalidated?

In-scope Citco entities do not use the Privacy Shield[2] and so Citco has historically avoided reliance on the Privacy Shield when it was offered as a data transfer mechanism by US-based service providers, vendors and other related counterparties. As a result, the invalidity of the Privacy Shield does not impact Citco entities.

4. How is the use of EU Commission Standard Contract Clauses (SCCs) now qualified?

As a result of the Schrems II ruling, a factor for relying on SCCs for ongoing and future cross-border data transfers outside the EEA is the need to evaluate the laws (in particular the surveillance laws) of the jurisdictions of recipients. This obligation rests with the exporter of the personal data.

From a US perspective, to determine whether an entity comes within the scope of surveillance law, the following surveillance law questions should be asked:

a. Direct application of Title 50 US Code § 1881a (Procedures for targeting certain persons outside the United States other than United States persons) (also referred to as FISA 702)?

   Does the recipient fall within one of the following definitions?

   (i) *"Telecommunications carrier"* as defined in section 153 of title 47 of the US Code (U.S.C.)?

   (ii) *"Electronic communication services"* as defined in section 2510 of title 18 U.S.C.?

   (iii) *"Remote computing service"* as defined in section 2711 of title 18 U.S.C.?

b. Processing data under Executive Order 12.333 (United States intelligence activities) (also referred to as EO 12.333)?

   (iv) Does the recipient that processes personal data it receives from the exporter, co-operate in any respect with US authorities conducting surveillance of communications under EO 12.333? If it does, is it mandatory or voluntary?

A US entity (looking to rely on SSCs) that comes within the scope of one or more of the definitions above will result in the use of SCCs being problematic or invalid.

However, according to the CJEU, there is a possibility that, even if US does not offer an "adequate" and "equivalent" level of protection in relation to government access to data, transfers can still take place if the data controller puts in place *"additional safeguards"*, *"additional measures"*, *"supplementary measures"* or "effective mechanisms to make it possible in practice" to ensure the protection of the data transferred by other means.

2 The service areas of Citco do not come within the supervisory remit of the US Federal Trade Commission, Department of Transportation and related bodies and as a result was not eligible to rely on the Privacy Shield as a basis for its own EEA-US cross border personal data transfers.

In its FAQ document released shortly after the Schrems II ruling, the European Data Protection Board stated that it is *"looking further into what these supplementary measures could consist of and will provide more guidance"*.[3]

Unhelpfully, to date, European Commission, European Data Protection Board and supervisory authority guidelines and practice directions have not been released to clarify what could be considered "supplementary measures". **However, it is widely thought (including, among others, Max Schrems himself in interviews and commentaries following the CJEU ruling) that the use of encryption practices (in transit and at rest), particularly with respect to US based cloud storage providers or other US based providers that do not need to "see" the personal data, would be considered an effective supplementary measure.**

The result of the Schrems II ruling is that it is not possible to use SCCs where the US recipient entity is subject to the relevant US surveillance laws and no supplementary measures will be put in place. In that instance, alternative cross-border data transfer mechanisms should be considered.

5. Does Citco rely on SCCs for its cross- border personal data transfer activities?

Where possible, in-scope Citco entities look to rely on SCCs for cross-border transfers. SCCs as a cross-border data transfer mechanism are the most widely adopted method by organisations for transferring personal data outside of the EEA. It is estimated that 89% of EU organisations rely on SCCs to cover their data transfers to the US and more than 80% rely on SCCs for their international transfers generally.[4]

6. Is Citco's use of SCCs for intra-group personal data transfers impacted by the Schrems II ruling?

The key determinant is whether or not the recipient US Citco service entity (the importer of personal data coming from the EEA) comes within the scope of the US surveillance laws that are highlighted in the answer to question 4 above.

Citco's US service entities do not fall within those definitions meaning that they are not subject to the US surveillance laws referred to in the Schrems II ruling. Therefore, SCCs already in place between in-scope Citco entities and Citco's US service entities are not qualified and continue to be valid without impact.

3 Source: Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en).

4 Source: 2016 IAPP Annual Privacy Governance Report, International Association of Privacy Professionals.

7. Is Citco's use of SCCs for client service relationships impacted by the Schrems II ruling?

The key determinant is whether or not the recipient entity (the importer of personal data coming from the EEA) comes within the scope of the US surveillance laws that are highlighted in the answer to question 4 above.

Generally speaking, the clients of in-scope Citco entities are not subject to the US surveillance laws referred to in the Schrems II ruling. Therefore, SCCs in place between in-scope Citco entities and clients are not qualified and continue to be valid without impact.

8. Is Citco's use of SCCS when relying on US based vendors/suppliers impacted by the Schrems II ruling?

The key determinant is whether or not the recipient entity (the importer of personal data coming from the EEA) comes within the scope of the US surveillance laws that are highlighted in the answer to question 4 above.

In-scope Citco entities are currently liaising with their US based vendors/suppliers and related parties (i.e. their sub-processors) to determine whether any of those vendors/suppliers are subject to the relevant US surveillance laws. Any US based vendors/suppliers relationships identified as in-scope will require, for ongoing and future transfers, that supplementary measures (encryption and/or other measures recommended by the EU Commission, European Data Protection Board or supervisory authorities) will be implemented as soon as possible or an alternative cross-border transfer mechanism be relied upon.

It should be noted that as part of Citco's data protection and information security measures, Citco relies on encryption as a non-contractual safeguard for cross-border transfers to the US and other third countries. Such encryption practices extend to (to the fullest extent possible) encryption in transit, at rest and the retention of encryption key(s). Encryption can make it more difficult for law enforcement (including surveillance authorities) to access data received in recipient countries, while at the same time protecting user data from criminal hackers. Based on the limited guidance available to date[5], the encryption practices adopted by Citco together with its use of SCCs results in Citco being able to continue to use and rely upon US based vendors/suppliers in a way that is compliant with the Schrems II ruling.

5 On 16 July 2020, the Data Protection Authority in Rhineland-Palatinate, Germany, indicated that there was no grace period for companies using the SCCs to comply with the CJEU requirement of essential equivalence standard and, if transferring unencrypted data to the U.S. and there are no other alternative data transfer mechanisms, those transfers are no longer possible. (https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/paukenschlag-eugh-schreddert-den-privacy-shield-datenuebermittlung-in-staaten-jenseits-der-eu-aber/