Confirmit Update:
International Data Transfers under the GDPR in the context of new EDPB Recommendations, new EU Commission SCCs, and Brexit

About this document: ***This document is intended to share Confirmit's understanding of the subject matters. This document must not be interpreted as legal guidance or advice.***
Given both EDPB Recommendations and EU Commission SCCs are still in consultation phase, interpretations may need to be updated later.
Links to external sites are provided for your convenience, Confirmit is not responsible for the content therein.

Since May 25th 2018, Regulation (EU) 2016/679 (the "**GDPR**") governs the processing of personal data in the countries belonging to the European Union ("**EU**") and to the European Economic Area ("**EEA**"), as well as storage and processing of personal data on behalf of EU and EEA citizens in countries outside of the EU and EEA. The GDPR defines requirements that must be met for personal data to be lawfully stored, or lawfully processed from, outside the EU and the EEA. This document addresses such processing or storage. Use of the following terms shall have the meaning attributed to those terms in the GDPR: personal data, (data) processor, (data) controller and processing.

1. Confirmit's compliance structure for international data transfers ("IDTs")

The structures we have in place at Confirmit[1] in relation to IDTs, have been developed by, and are constantly being updated in close cooperation with, external privacy lawyers who are considered experts in the field. Contractual agreements have been executed between all Confirmit entities (intra-group data transfer agreements) enabling lawful transfer and processing of personal data by all such entities. Additionally, we have in place, as required, agreements with third parties acting as sub-processors on Confirmit's behalf in relation to our customers' personal data.

The back-bone of all such agreements are the EU Standard Contractual Clauses ("**SCC**"s).

2. Several developments impacting IDTs

In this document we will focus on 5 main areas which have recently undergone or are undergoing changes in relation to IDTs.

a) US / EU (and Switzerland) Privacy Shield no longer valid

Privacy Shield is a mechanism agreed to between the US, the EU and Switzerland, and which permits transfers of personal data to, and processing of personal data from the US. The Court of Justice of the European Union ("**CJEU**") however invalidated the Privacy Shield in July 2020 (the "**Schrems II**" case).

Confirmit remains registered under Privacy Shield, but does not rely, and has never solely relied on, the Privacy Shield for IDTs to the US. We rely on the SCCs, which remain valid, see item b) below.

b) SCCs remain approved method of transfer, but….

Under the GDPR, the SCCs remain a valid transfer mechanism to "**third countries**" (defined as countries

[1] References to Confirmit in this document include reference to Dapresy.

outside the EEA and other than countries deemed to be adequate by the EU[2]). SCCs were not invalidated by the CJEU ruling of July 2020. However, the CJEU introduced a requirement for data controller / data exporter, and data processors / data importers, to assess whether additional safeguards (renamed to "supplementary measures" in the European Data Protection Board **("EPDB")** Recommendations, see item 2 c) below) would have to be put in place for continued reliance on the SCCs. The CJEU however did not provide guidance in relation to what such supplementary measures would entail in practice for controllers and processors until November 2020.

c) In November 2020, the European Data Protection Board provided guidance "on measures that supplement transfer tools to ensure compliance with the EU (EEA) level of protection of personal data" (not yet finally approved).

On November 11th, 2020 the EDPB published long awaited guidance, to address some of the requirements for continued reliance on the SCCs. Two documents were released:

1. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"
    - Includes 6 steps procedure – please see infographic at the end of this document.
2. "Recommendations 02/2020 on the European Essential Guarantees for surveillance measures"

Both of the above are available at this link. The document in item 1. above was in consultation mode until 21 December 2020 and final EDPB approval and publication is expected in Q1 2021.

d) The European Commission has released new SCCs (not yet finally approved).

On November 12th, 2020 the EU Commission published 2 sets of documents:

1. "Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries", available here
2. "Commission Implementing Decision on standard contractual clauses between controllers and processors located in the EU", available here

Both of the above documents were in consultation until 10 December 2020. Final EU Commission approval and publication is expected for Q1/Q2 2021. In relation to item 2 d) 1 above, in the Appendix to the Implementing Decision, the EU Commission has consolidated into one document the two previous SCC sets respectively from 2004 (Controller to Controller) and 2010 (Controller to Processor) and has extended the framework with two more scenarios, Processor to Controller and Processor to (sub)Processor.

The EU Commission grants companies one year[3] from the date of "entry into force" of the decision, to update their currents SCCs with new ones, so that will likely give companies up to early 2022 to act.

e) Brexit.

Since January 31st, 2020, the UK is no longer a member of the EU. However, until December 31st, 2020, the UK operated under transitional terms with the EU/EEA which, for all practical purposes, meant that the UK was treated as a EU member in relation to EU law including in relation to data protection and international data transfers.

On January 1st, 2021, the transition period ended. However, on December 24th, 2020, the EU and the UK signed a Trade and Cooperation Agreement ("**TCA**"). This 1256-page agreement ensures continued, orderly trade relationships between those parties. The EEA countries accede to those terms in parallel.

The TCA includes "*Article FINPROV.10A TCA [4] - Interim provision for transmission of personal data to the United Kingdom*". This provides another transitional period, referred to as the "specified period", in relation to

[2] Reliance on adequacy is not affected by the EDPB guidelines, see EDPB Recommendations section 19.

[3] Article 24 of the Implementing Decision of the SCCs.

[4] https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-857-F1-EN-ANNEX-1-PART-1.PDF

data protection and international data transfers involving the UK. The specified period will last up to 6 months, e.g., until the end of June 2021. This will allow personal data to flow freely between the EU and the UK without the need for additional transfer mechanisms as the UK will not be considered a third country for data export purposes during this period.

The expectation is that the EU and the UK will be able to reach agreement on approving the UK as an adequate country (see item 2 b) above). Assuming this happens, processing of personal data in or from the UK, would for all practical purposes be the equivalent to such processing taking place within the EU/EEA. This would for example mean that Confirmit customers operating in the EU/EEA and storing / processing data on the UK based Confirmit SaaS, are not required nor eligible to enter into the SCCs referred in item 2 d) 1 above.

For Confirmit customers located in Norway (within the EEA but outside the EU), the Norwegian government has issued formal regulation[5] to align Norway with the TCA terms. As such, no action is required by Norwegian companies in relation to Brexit for the time being.

3. What does the EDPB now require data exporters to do?

Confirmit's Chief Legal Officer & Data Protection Officer is ensuring that Confirmit team members, alongside external lawyers and advisors, are taking all required steps to properly understand and follow the legal and operational implications of the EDPB Recommendations, the new EU Commission SCCs, and future Brexit developments.

Each data exporter is now required to follow a roadmap to see if it needs to put further measures in place before exporting personal data. The mapping process is set out on the infographic on the last page and entails two main focuses:

Firstly, determine whether the country in which personal data will be processed meets the requirements of the EDBP's newly released "*European Essential Guarantees for surveillance measures*". Four sets of guarantees would have to be present in that country:

- Processing should be based on clear, precise, and accessible rules.
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated.
- Independent oversight mechanism.
- Effective remedies need to be available to the individual.

Assessing the above requires understanding the laws relevant to the transfer, and not "all" laws. To the extent the laws prove to provide essentially equivalent level of protection to the GDPR, the transfer can proceed under currently available GDPR transfer mechanisms (such as SCCs).

Secondly, should the foregoing analysis determine that such guarantees are not in place in that country, then the EDPB Recommendations and the new EU Commission SCCs make it clear that IDTs can still take place, assuming however that supplementary measures can reliably be put in place. These supplementary measures fall into three categories:

- Contractual
- Technical
- Organizational

Please do however note that since the guidelines / recommendations from the EDPB are yet not officially published after the consultation period ended, some changes may find their way into the final version.

[5] https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/overforing-av-personopplysninger-til-storbritannia-kan-fortsette-som-for/

4. What has Confirmit done?

Firstly, Confirmit has already taken measures to strengthen the security of its data in relation to potential US access, specifically (i) whilst data on the UK server remains stored on that server, the US arm of our hosting provider was previously able to access the raw data (without links to the survey itself) for the purpose of supporting the system, particularly out of hours. A new stricter procedure has been introduced under which the hosting provider no longer has default access. Should it be absolutely necessary for it to have access, it is now only available under strictly controlled time limited conditions and (ii) a system has been implemented such that clients may specify that technical support users and consultants outside of the EU / EEA no longer have access to their data. However, it is important to note that there may be a small delay in resolving technical support queries if this option is chosen by our customers.

A secondary suggested process enhancement by the EDPB is to implement encryption, however we have for some time encrypted the data both at rest and in transit, so that precaution is already in place.

Thirdly, Confirmit has initiated assessment processes for both focuses in Item 3 above. The outcome of our assessments will be made available to our customers later, after the EDPB Recommendations and the new EU SCCs have been rendered "final". Confirmit's documentation will include listing of relevant supplementary measures (implemented or planned).

The assessments which Confirmit is currently working on include:

A. Assessment of third country laws "relevant to the transfer":

Confirmit has procured external legal guidance to assess whether the laws of the third countries in which Confirmit stores personal data, or from which personal data is accessed remotely, provide the data subjects a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR. The guidance is specific to Confirmit's activities and roles, thus confidential to Confirmit and is therefore not shared with customers. The findings of the guidance will form the basis for the supplementary measures Confirmit will put into place to align with the new EDPB Recommendations and this would be shared with our customers, as appropriate. Customers are advised to obtain their own assessments by their own legal resources.

B. Contractual measures:

As soon as the new SCCs are published by the EU Commission as being "final" , Confirmit will initiate processes to enter into those new and updated sets of SCCs with Confirmit sub-processors who are involved in the processing of personal data on behalf of Confirmit's customers. As an alternative to signing new SCCs, to the extent permissible by law, addenda may be entered into instead if such approach would align with the new requirements.

Confirmit will also provide its customers with guidance in relation to signature between customer and Confirmit of new SCCs.

C. Technical and Organizational measures:
The effect of the contractual and operational relationship between Confirmit and its hosting provider for the SaaS hosting environment (currently Rackspace Ltd UK), being controlled by Confirmit AS, Norway (within the EEA), and not by Confirmit entities outside of the EEA, is to be considered.

Confirmit will further ascertain the relevance of the descriptions provided by the EU Commission in the final SCCs, in Annex III "*Technical and organisational measures including technical and organisational measures to ensure the security of the data*".

5. Do Confirmit customers need to sign any new IDT related agreements with Confirmit NOW?

In relation to Brexit: No.
We do always encourage our customers to take independent legal advice in relation to its own organisational requirements.

Confirmit will continue to monitor development throughout the six-months period through end of June 2021 and will provide updated status later.

In relation to the new SCCs: No.
We do always encourage our customers to take independent legal advice in relation to its own organisational requirements.

There are presently inconsistencies between the draft recommendations issued by the EDPB and the draft SCCs issued by the Commission. Therefore, Confirmit deems it premature to start any renegotiation of agreements related to IDTs with its customers. We await the EU Commission's publication of the final version of the SCCs, alongside the EDPB publication of the final version of the guidelines. Based on those, we will assess the appropriate path forward. We will do our best to put together models that can reduce the burden on our respective teams and ensure that we all will continue to operate in compliance with applicable laws and guidance.

Confirmit believes that it has taken prompt action to respond to the new guidance issued and, as before, intends to remain compliant with GDPR law.

As ever, we encourage our customers to obtain individual legal advice in relation to its business needs and requirements in this area.

Source: https://twitter.com/EU_EDPB/status/1326538247980249092?s=20