EU 2021 STANDARD CONTRACTUAL CLAUSES (SCCs) AND UK 2022 SCCs: FAQ FOR ACCENTURE SUPPLIERS.

This SCCs FAQ is intended to assist Accenture's Suppliers in understanding Accenture's approach to personal data transfer compliance. **This SCCs FAQ does not constitute legal advice from Accenture – suppliers must obtain their own independent legal advice.**

1.	**What are Standard Contractual Clauses ("Prior SCCs")?** ➡ These are contractual clauses typically attached to Data Protection Agreements or Schedules under which a recipient of personal data in a third country agrees to protect the information received in accordance with 2016/679 General Data Protection Regulations ("GDPR").
2.	**What are the New/2021 Standard Contractual Clauses ("New SCCs")?** ➡ In June 2021 the European Commission published a decision regarding the New SCCs for GDPR compliant transferring of personal data from the European Union to third Countries. ○ The New SCCs clarify the necessary steps for transferring personal data to third Countries. ○ The New SCCs aim to resolve the practical issues arising from the Prior SCCs. The aim of the New SCCs is to align with "GDPR" as well as clarifying what data exporters and data importers need to assess. ○ The New SCCs also spell out what further steps need to be taken to ensure the same level of protection is afforded to personal data in the importing country as is provided in the EU. ○ The UK's new International Data Transfer Agreement ("IDTA"), and new International Data Transfer Addendum ("the UK Addendum") to the New SCCs are essentially the UK version of the new SCCs. The UK Addendum to EU SCCs permits reliance on EU SCCs for UK transfers.
3.	**What is the deadline for implementing the New SCCs?** ➡ Contracts that incorporate Prior SCCs will remain valid until the end of **27 December 2022**, after which time the New SCCs must be entered into in replacement of the Prior SCCs.
4.	**What are they key points from the Schrems II decision which resulted in the New SCCs?** ➡ The decision struck down Privacy Shield, a mechanism allowing for the exchange of personal data between the EU/EEA and the US. The New SCCs clarify the necessary steps for transferring personal data to third Countries. ○ The result of this was that many organisations transferring personal data to the US could, from then on, only transfer personal data by means of employing SCCs. ○ The Prior SCCs were upheld as a valid means of exchanging personal data with a third country however, The Court of Justice of the European Union ("CJEU") stressed that organisations must, verify that EU personal data being transferred outside of the EU will be adequately protected in the destination country in line with the level of protection set out in the GDPR. ○ The Schrems II decision resulted in uncertainty regarding how to legally transfer personal data outside of the EEA, notwithstanding that the SCCs were upheld. There was a particular concern as to whether the risk-based approach to assessing a destination third country's local law would be maintained.
5.	**Key improvements in the New SCCs:** ➡ **Modular clauses:** This effect of the modular approach will be of a huge practical benefit. Rather than having different SCCs for different relationships between exporters and importers, there is now one set only, with 'modules' to be applied as is appropriate to the relationship in question. This shift away from the previous separate sets of clauses, is welcome as the old approach failed to recognize the complexity of modern data processing chains. ➡ **Docking clause:** Clause 7 enables third parties to accede to the agreement at any point in time provided the existing parties are all in agreement. This is a major improvement on the Prior SCCs, which would have required a new or additional agreement to be re-executed. ➡ **Onward transfers:** Clause 8 prohibits onward transfers of personal data to a third party located outside of the EEA unless that party agrees to be bound by the New SCCs. There are a number of exceptions to this including where express consent of the data subject is obtained or where it is necessary in the case of a legal claim.

6.	**What is the process to sign New SCCs? Who should sign these clauses?** ➡ Accenture is conducting a suppliers' remediation process by sending a SCC Amendment to remediate supplier contracts under which EEA, UK, Swiss personal data is transferred to non-adequate countries. The Amendment contains Attachments related to EEA, UK and Swiss personal data transfers. The Amendment includes mandatory clauses, and it is ready to execute by suppliers. The New SCCs are mandatory to execute, and they should be accepted by the Parties "as is" in order to be valid.
7.	**What is a Transfer Impact Assessment ("TIA")?** ➡ Data exporters and data importers cannot simply say that the New SCCs apply and take no further action. Clause 14 requires Parties to consider: ○ the nature of personal data transferred and purpose for processing; ○ the law and practice of the third country; and ○ any relevant contractual, technical or organisational to supplementary measures implemented. ➡ A TIA must be made available if requested by a competent supervisory authority. The TIA will help to ensure that personal data being transferred to a third country will be adequately protected in the destination country in line with the level of protection in the EEA/UK/Switzerland. ○ The TIA will require information regarding the circumstances of the transfer of personal data and the relevant laws and practices of the third country. ○ If the personal data being transferred to a third country is not adequately protected in the destination country the TIA will assist in identifying the necessary adequate, technical, organizational or contractual supplementary safeguards to align the level of personal data protection with the EU standard, if possible. ○ In June 2021, the European Data Protection Board ("EDPB") finalised its recommendations on supplementary safeguards for personal data transfer tools to ensure compliance with the EU standard of personal data protection ("EDPB Recommendations"). ○ The EDPB Recommendations examine the obligations of EEA Personal Data exporters and importers in relation to the TIA and supplementary safeguards and provides detailed recommendations in connection thereof. ○ Swiss and UK data protection authorities have agreed to follow the EDPB Recommendations with regard to data transfers. UK ICO (The Information Commissioner's Office) defined Transfer Risk Assessments (TRAs) process which is similar to TIA.
8.	**Who is responsible for conducting a Transfer Impact Assessment?** ➡ The data exporter has the primary responsibility for conducting the TIA (irrespective of their role as a controller or processor in the personal data processing involved). The data importer has an obligation to collaborate with the data exporter within the TIA process. There are some questions in TIA which need supplier cooperation and input and it is the supplier's obligation to collaborate with Accenture being data exporter in order to complete the TIA.
9.	**Who is a Data Exporter?** ➡ The entity 'exporting' the personal data outside the EEA, UK, Switzerland i.e. operationally transferring (including providing access to) Accenture or Accenture client personal data or contractually engaging the data importer to process personal data in a third country. The data exporter can be either based within the EEA, UK, Switzerland or be based outside EEA, UK, Switzerland, regardless they are subject to the GDPR. The data exporter may be a data controller, a data processor or a sub-processor.
10.	**Who is a Data Importer?** ➡ The entity located outside the EEA that receives personal data ,for processing or accesses, which is protected under the GDPR. The data importer may be a data controller, a data processor or a sub-processor.
11.	**What does it mean EEA?** ➡ The European Economic Area, integrated by the Member States of the EU (see http://europa.eu/about-eu/countries/ for an up-to-date list of Member States) plus Norway, Iceland and Liechtenstein.
12.	**What are Supplementary Measures?** ➡ Technical or organizational (for example, encryption, data minimization, greater access controls or potentially key management changes) or contractual/legal (for example, additional contract clauses to protect personal data) measures aimed at ensuring, on a

	case-by-case basis, that transferred personal data is granted an essentially equivalent level of protection in the third country compared to that provided in the EEA. These measures shall be selected by data exporter, depending on the outcome of the TIA carried out, also considering the European Data Protection Board (EDPB) Recommendation 1/2020 on supplementary measures, finalized on 18 June 2021. Accenture applies supplementary measures based on TIA scoring and they are attached to the remediation Amendment.
13.	**What are third countries?** ➡ For the purpose of EEA, UK, Swiss data transfer any country outside the EEA other than adequate countries, to which personal data is transferred. ○ Adequate counties are the countries outside the EEA which have been granted an "adequacy" status by the EU Commission. They include Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, the State of Israel, Isle of Man, Japan, Jersey, New Zealand, Uruguay, UK and the transfer of Air Passenger Name Record to the United States' Bureau of Customs and Border Protection and to the Australian Customs Service. An up-to-date list of the non-EEA adequate countries can be found here.
14.	**What are requirements for personal data transfer from UK?** ➡ On March 2021, the Information Commissioner's Office (ICO) released two new transfer tools for compliance with UK GDPR when making restricted data transfers from the UK to third countries (non-adequate countries): (i) The UK's new International Data Transfer Agreement ("IDTA"), and new International Data Transfer Addendum ("the UK Addendum"). You can find more information HERE. ➡ **21 March 2022** IDTA & Addendum came into force. Accenture applies The UK Addendum to EU SCCs which permits reliance on EU SCCs for UK transfers. ○ For contracts concluded on or before **21 September 2022**, the legacy SCCs can continue to be used, but only where there is no change to the processing operations and that existing contracts ensures adequate safeguards in compliance with Schrems II.
15.	**How personal data are transferred from Switzerland?** ➡ The Federal Data Protection and Information Commissioner ("FDPIC") has recognized the new SCCs approved by the EU Commission as a valid mechanism for data transfers to third countries that do not offer adequate data protection subject to Swiss law (currently, the Federal Act on Data Protection 1992). Therefore, as of 27 September 2021, when a data exporter based in Switzerland is going to transfer EEA personal data (also together with Swiss personal data) outside its country, the new SCCs shall be used. ○ As it was made in Attachment to the remediation Amendment, there is a need to adjust the SCCs template according to the guidelines provided by the FDPIC in its paper "*The transfer of personal data to a country with an inadequate level of data protection based on recognised standard contractual clauses and model contracts"* published on 27 August 2021, available here.
16.	**The clause 13 (Supervision) of SCCS.** ➡ The Clause 13 included in Module 1 C2C, Module 2 C2P and Module 3 P2C - contains three options, one of which must be selected by data exporter for the purpose of identifying which supervisory authority within the EEA will be competent to oversee the compliance with the SCCs by the signatory parties. Please note that also Annex I.C of SCCs is referring to Competent supervisory selected in Clause 13 of SCCs. ○ Options are specific to the following data exporter situations: 1. Data exporter is established within the EEA; 2. Data exporter is established outside the EEA but is nevertheless subject to the GDPR and has appointed an authorized representative in the EEA pursuant to Art. 27 GDPR; 3. Data exporter is established outside the EEA but is nevertheless subject to the GDPR and has NOT appointed an authorized representative in the EEA pursuant to Art. 27 GDPR. In the Amendment Option 1 is selected by default but it can be changed by supplier being data exporter. Options 2 and 3 refer to cases where the non-EEA data exporter is entrusting a data importer with processing activities related to EEA personal data.