Third Country Transfers Module

Explanatory note

September 2023

1 Introduction

The Third Country Transfers Module (referred to as the "**Module**") is designed to address the uncertainties surrounding international data flows for cloud service providers (the "**CSPs**") in the wake of the Schrems II ruling. Its objective is to provide a legal framework and certainty for the cloud sector by structuring the discussions around international data transfers and incorporating the requirements derived from the European Data Protection Board (EDPB) Guidelines and Schrems II ruling. The module aims to create coherence in the cloud market, as well as for controllers and data subjects.

The intent is to safeguard personal data transferred to third countries in accordance with the GDPR, by establishing adequate standards for transparency and accountability of CSP and facilitating compliance assessments of services provided by adherent CSPs. The Module does not re-allocate legal obligations and accountability between processors and controllers. Therefore, as established by the GDPR, it is up to each controller to determine in its sole discretion whether or not there are appropriate safeguards for a data transfer, having conducted suitable due diligence and considered the input of its processor, the CSP.

This explanatory note will outline the guiding principles that have shaped the development of the Module, its structure, and key elements.

2 Guiding drafting principles

2.1 Relationship with EU Cloud Code of Conduct

The Module builds upon the EU Cloud Code of Conduct (the "**EU Cloud CoC**") and requires CSPs to comply with it as a prerequisite. However, the Module should be regarded as a distinct code of conduct pursuant to Article 40 GDPR requiring independent approval as outlined in the GDPR. While the EU Cloud CoC includes a set of requirements that enable Cloud Service Providers to demonstrate their capability to comply with their role as a processor (Article 28 GDPR), the Module covers the legal requirements for third country transfers as outlined in Chapter V of the GDPR.

2.2 Processor's Code

As is the case for the EU Cloud CoC, this Module only applies to "business-to-business" (B2B) cloud services where the CSP is acting as a processor. It therefore does not apply to "business-to-consumer" (B2C) services or for any processing activities for which the CSP may act as a data controller. While there is no reallocation of responsibilities, the aim is to impose standardized mechanisms through which CSPs can effectively support customers and controllers.

2.3 Annexes and Templates

The Module aims to create coherence and increase transparency in the cloud sector by introducing standardized templates and easy-to-recognize formats. These templates will facilitate compliance with documentation and communication requirements. The main annexes include the Transfer Impact Assessment Transparency Document (the "**TIAT Document**"). It aims at enhancing transparency by offering clear communication of applicable situations and the implemented Supplementary Measures (as defined in the Module). This template is still to be drafted based on the requirements of **section 4.2 "Transfer Impact Assessment"** of the Module.

2.4 Incorporating EDPB Guidelines and Schrems II Ruling

The Module aims at incorporating all the relevant requirements derived from the EDPB Guidelines/Recommendations and the Schrems II ruling. However, it specifically focuses on translating these requirements into obligations suitable for processors.

2.5 Beyond SCCs and BCRs

In light of the recent developments relating to international data transfers, it is crucial to explore measures that go beyond typically those included in Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs). While SCCs and BCRs have traditionally been instrumental in ensuring data protection in cross-border transfers, emerging privacy concerns and legal challenges necessitate additional measures and guidance for achieving GDPR-compliant third country transfers.

The purpose of this Module is to enhance legal certainty by establishing a systematic approach for conducting assessments by CSP. Additionally, this module addresses the additional requirements that are in EDPB guidelines, which go beyond the SCCs. By that it encompasses additional commitments, such as training and notification obligations, set forth by data protection authorities.

Therefore, the Module aims to offer an elevated level of legal certainty, transparency, and accountability to meet the evolving requirements in the field of data transfers.

2.6 Structural presentation

The Module consists of a set of obligations which are to be referred to as "Controls". Relevant Controls have been integrated throughout the text of Module and enumerated in section numbers, so that any interested party can easily determine the requirements of the Module that must be implemented in practice. The Controls are thus an inherent part of the Module, and compliance with the Controls is a mandatory part of declaring adherence to the Module. In addition, background explanations and context are provided in the blue boxes and implementation guidance in the green boxes. As such, the

guidance is not binding, and CSPs may implement Controls in a different manner that achieves the same outcomes. However, the guidance provides a certain level of support for CSPs who are uncertain on how to interpret and implement Controls.

3 Explanation on the structure of the Module

CSPs must comply with **Section 4 "Requirements"** which sets out Controls and guidance to help CSPs manage their policies and processes to achieve compliance with the Module.

The first part, which is **section 4.1 "General Obligations"**, relates to the general data protection principles that must be in place and which are derived from the Guidelines 04/2021 on codes of conduct as tools for transfers from the EDPB. This section covers principles such as transparency, fairness and lawfulness, purpose limitation, data minimization and accuracy, limited storage of data, processing of sensitive data, security, compliance with instructions from the controller (for processors), including rules on the use of processors or sub-processors, and rules on onward transfers. Whenever those elements are covered by the EU Cloud CoC, the Module simply refers to the relevant sections. While many of these principles relate to what is typically covered by SCCs, the section aims to provide additional legal certainty. Therefore, it includes measures that go beyond what is included in SCCs to also address - when relevant - the specific recommendations provided by the EDPB. By including these measures, the module seeks to enhance data protection standards and withstand scrutiny from data protection authorities.

The second part which is **section 4.2 "Transfer Impact Assessment"** constitutes the core of the module as is it introduces the methodology for CSPs when it comes to assessing the impact and security implications of a third country transfer. Therefore, it covers the following:

- identifying and documenting factors such as laws or practices applicable to the third country transfer and determining whether the implementation of Supplementary Measures are necessary to guarantee a level of data protection equivalent to that ensured within the EU by GDPR; and
- assessing and identifying the adequate Supplementary Measures.

To document this assessment the Module sets-forth the **TIAT Document** which is composed of the following two templates:

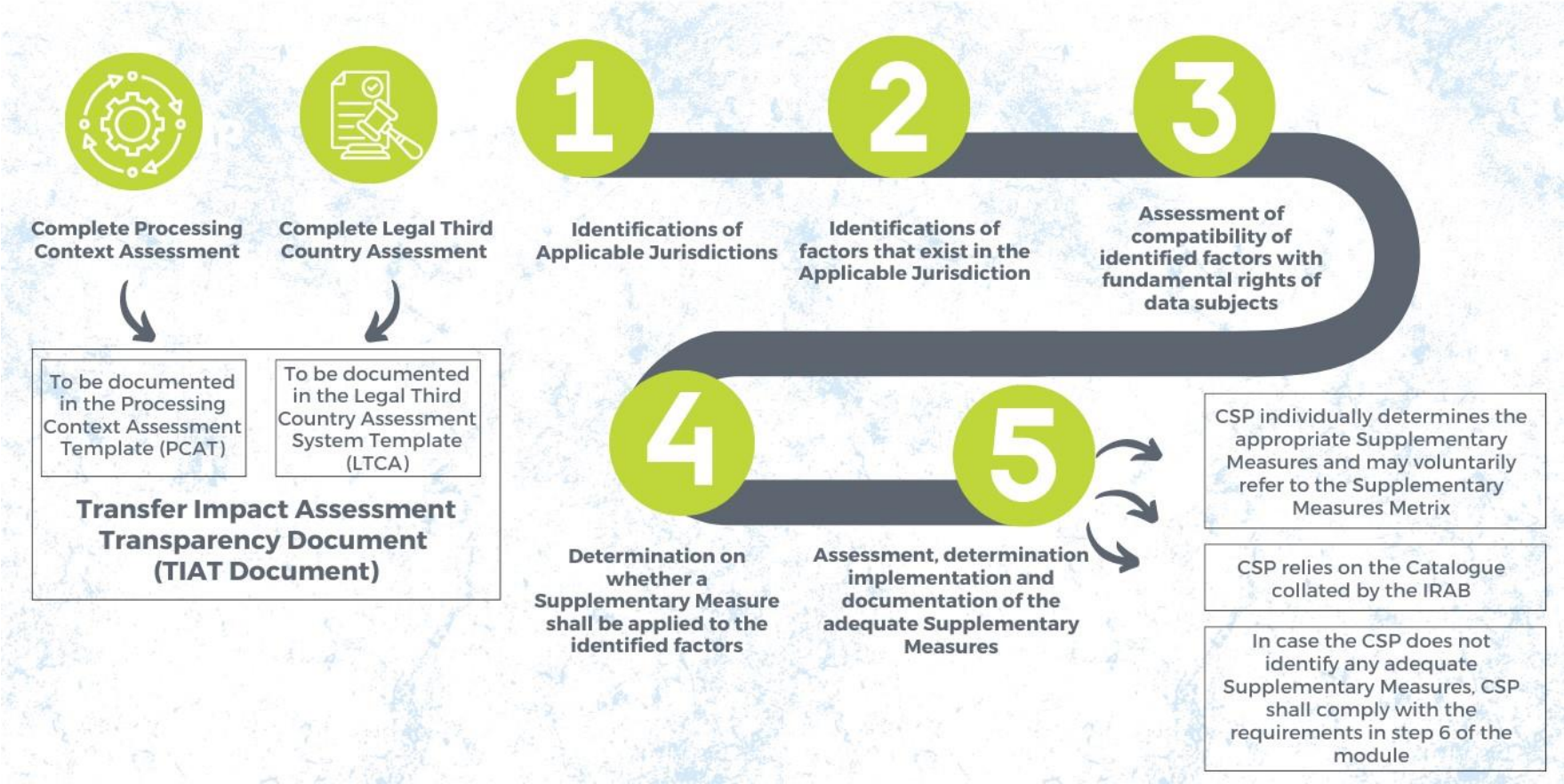
- **Processing Context Assessment Template** (**PCAT**) which focuses on documenting for instance, the type and format of processing taking place and whether there is any onward transfer.

- **Legal Third Country Assessment System** (**LTCA**) involves documenting factors such as laws and practices applicable to the third country transfer. It also entails determining whether Supplementary Measures need to be implemented and, if required, identifying the suitable Supplementary Measure.

The **TIAT Document** is to be completed by the CSPs and submitted to the Monitoring Body.

The flowchart that follows outlines the various steps that CSPs must take to comply with section 4.2 "**Transfer Impact Assessment**" and that must be documented in the TIAT Document.

Transfer Impact Assessment



3.1 The Supplementary Measures Matrix

Whenever the CSP decides in accordance with step 5 above to individually determine the appropriate Supplementary Measure, the CSP may rely on the Supplementary Measures Matrix which will be annexed to the Module.

This matrix shall provide an inventory of Supplementary Measures that are typically applied when a certain risk factor is identified. Structurally speaking the matrix links Supplementary Measures with factors in third countries that may impose risks.

It is important to note that the matrix will serve as guidance only, and it is at the discretion of the CSP to decide whether or not to implement the listed Supplementary Measures. As a result, CSPs may choose to apply different Supplementary Measures that they deem suitable.

3.2 The Catalogues and the IRAB

As shown in the diagram above, the CSP has the option to rely either on the Supplementary Measures Matrix or the catalogues to guide them in the determination of the appropriate Supplementary Measure. If the CSP determines that its Processing Context (as defined in the Module) aligns with the one provided in a catalogue compiled by the Independent Risk Advisory Body (IRAB), it can choose to implement the Supplementary Measures listed in that catalogue.

The IRAB shall be an independent body which co-operates with the Monitoring Body, as well as potentially with the competent supervisory authority within the framework of the Module to develop and update catalogues that determine an adequate selection of risk-related Supplementary Measures for a specific Processing Context. Such catalogues are intended to support a CSP and subsequently their customer to implement appropriate Supplementary Measures. The Module foresees a dedicated process that gives – at a minimum – the competent supervisory authority a say on this developed catalogue. The latter would significantly underpin the positive effect and rigor of codes of conduct as a safeguarding mechanism and provide the desired legal certainty.

About EU Cloud CoC

The EU Cloud Code of Conduct is an approved and fully legally operational Code of Conduct pursuant to Article 40 GDPR. Defining clear requirements for Cloud Service Providers to implement Article 28 GDPR, the Code covers all cloud service layers (IaaS, PaaS, SaaS), has its compliance overseen by an accredited monitoring body, and represents the vast majority of the European cloud industry market share.