Third Country Transfers Module - DRAFT

DRAFT | v 0.4

September 2023

Disclaimer

This document is a draft version of the Third Country Transfers Module and is being published solely for the purpose of gathering stakeholder feedback. As such, it is not the final version and is subject to significant adjustments based on the feedback received from various stakeholders as well as ongoing internal discussions.

All individuals and entities who review this draft are encouraged to provide their input, suggestions, and concerns, as their feedback is crucial in shaping the final version of the Third Country Transfers Module.

It is essential to understand that any statements, provisions, or guidelines outlined in this draft are subject to change, deletion, or addition as part of the revision process. We will carefully consider feedback received and incorporate relevant modifications to produce a comprehensive and effective solution.

This draft version is not legally binding and should not be construed as an official representation of the opinions or statements of the members of the EU Cloud Code of Conduct. It is solely intended for informational purposes and to facilitate an open dialogue with stakeholders.

1 Introduction

This Third Country Transfers Module (as defined in Section 2 "Terminology"; short "Module") constitutes an on-top module of the main body of the EU Data Protection Code of Conduct for Cloud Service Providers (the "EU Cloud CoC"). It is interlinked with the existing EU Cloud CoC provisions and shall cover the legal requirements for third country transfers as outlined in Chapter V of the GDPR (as defined in Section 2 "Terminology"). As an on-top module, the Third Country Transfers Module is not a standalone initiative; compliance with the EU Cloud CoC is a pre-requisite. However, the Third Country Transfers Module should be regarded as a distinct code of conduct pursuant to Article 40 GDPR (i.e., it shall follow the independent approval process as specified in aforementioned article) and not as an amendment to the existing main body of the EU Cloud CoC.

This Third Country Transfers Module is intended to safeguard personal data transferred to third countries in accordance with the GDPR, by establishing adequate standards for transparency and accountability of Cloud Service Providers ("CSPs") and facilitating compliance assessments of services provided by adherent CSPs.

In particular, the Third Country Transfers Module shall be considered an appropriate safeguard when personal data is transferred outside of the European Union or and European Economic Area ("EU"/"EEA") pursuant to Article 46 GDPR. Thus, it can be utilized as a standalone appropriate safeguard under Article 46 GDPR by both the CSPs and their Customers.

Given the need for an instrument that is sufficiently flexible to address multiple jurisdictions, but that is also proportionate and comprehensive for companies to use, the Third Country Transfers Module creates an overarching, yet robust framework. This framework guarantees that third country transfers respond to the fast-paced dynamic of international markets and that data subjects are properly and uniformly protected in accordance with European standards. While no jurisdictions or data processing activities will be excluded up-front, when the standards and procedures required by the Third Country Transfers Module are applied, the result may be that the third country transfer cannot take place.

The Third Country Transfers Module refers to the provisions of the EU Cloud CoC, where relevant, and uses additional language, as necessary, to address the specificities and risks of third country data transfers.

The Third Country Transfers 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. However, particularly in the context of highly standardized Cloud Services, and thus standardized Cloud Service Agreements and technical and organisational measures, controllers require significant support from CSPs in order to complete this due diligence. This Module creates mechanisms by which CSPs can provide that support, including easily recognizable and useable templates to provide controllers and Customers with increased transparency about the technical and organisational measures implemented by CSPs. Thus, this Third Country Transfers Module will facilitate and optimize the due diligence of controllers and Customers.

The Third Country Transfers Module consists of a set of obligations which are to be referred as "Controls". Relevant Controls have been integrated throughout the text of this Third Country Transfers 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.

2 Terminology

Any terminology used in the Third Country Transfers Module that is defined by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation or "GDPR", as may be amended from time to time) (e.g. terms such as "personal data", "controller", "processor", "data subject", etc.) shall have the meanings given by that regulation and the EU Cloud CoC, unless explicitly stated otherwise.

Furthermore, the following defined terms are used in this Third Country Transfers Module:

- *Catalogue* means a collection of pre-selected supplementary measures determined to be suitable for a specific Processing Context, as prepared by the IRAB.
- *Customer has* the meaning defined in the EU Cloud CoC, and accordingly may refer to either a processor or controller.
- *IRAB* refers to the Independent Risk Advisory Body, as set out in Section 5.
- *May, can, should*, define optional elements. Such language may be used to explicitly clarify that related aspects remain possible, thus, that the Module does not affect compliance with any other laws than the Applicable Data Protection Laws and does not affect any activities outside the scope of this Module. This language may also be used in the context of guidance to mandatory requirements; in this context the optional is necessary to reflect the multitude of existing real-life scenarios by remaining flexibility, and where possible to provide examples of reference, from which relevant stakeholders and the Monitoring Body ("MB") can derive good practices and expectations of how the requirements should be implemented.
- *Onward Transfer means* a further transfer of personal data to a third party within the same or another Third Country after the data has been transferred to a Data Importer outside the EU or EEA in reliance on appropriate safeguards under Article 46 GDPR, in circumstances where a third party is not bound by the appropriate safeguards of the initial transfer.
- *Processing Context* refers to the nature of processing activities concerned in light of the applicable third country laws and practices. The nature of processing activities refers to parameters such as personal data processed, processing purpose, data subjects, processing (technical system) means and recipients of personal data.
- *Sub-Processor* means any processor directly engaged by the Cloud Service Provider.
- *Supplementary Measures* means additional technical, organisational and/or contractual safeguards that supplement the obligations imposed by the GDPR, in order to ensure that a

third country's legal system does not undermine the level of data protection required by GDPR.

- *Third Country* means any country outside of the EEA, and also comprises international organisations.
- *Third Country* Transfers *Module*, short Module, means this document including any Annexes and ancillary documents, such as Catalogues.
- *Third Country Transfer,* is a form of personal data processing that satisfies three cumulative criteria:

  1) A controller or a processor is subject to the GDPR for the given processing.

  2) This controller or processor ("Data Exporter") discloses by transmission or otherwise makes personal data, subject to this processing, available to another controller, joint controller or processor ("Data Importer").

  3) The Data Importer is in a third country or is an international organisation, irrespective of whether or not this Data Importer is subject to the GDPR in respect of the given processing in accordance with Article 3.[1]

[1] See *European Data Protection Board's Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (version after consultation Adopted on 14 February 2023).*

3 Scope

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. It also does not apply to scenarios where no Third Country Transfer takes place; in that case, the EU Cloud CoC would suffice to protect the personal data of individuals in line with the GDPR requirements.

This Module serves as an appropriate safeguard in both initial Third Country Transfers and Onward Transfers.

This Module qualifies as a transnational Code of Conduct meaning that it covers processing activities across state borders and as such requires to be submitted to the European Data Protection Board in accordance with Article 63 GDPR.

4 Requirements

This section sets out controls and guidance to help Cloud Service Providers manage their policies and processes to achieve compliance with the Third Country Transfers Module.

Those controls include general obligations provide safeguards that apply uniformly across all Third Countries, independent of the level of protection guaranteed in each Third Country. The controls also include a transparency system, which maps the specifics of a Cloud Service and of individual relationships between Customers and CSPs into operational and effective means, to facilitate each Customer's GDPR compliance when transferring Customer Personal Data to a specific Third Country. Finally, those controls include a legal third country assessment system for determining whether and which additional measures must be applied to a specific transfer.

4.1 General Obligations

4.1.1 Data Protection Principles

In accordance with Guidelines 04/2021 on Codes of Conduct as tools for transfers, a code of conduct shall include a description of the data protection principles to be complied with under the code (transparency, fairness and lawfulness, purpose limitation, data minimization and accuracy, limited storage of data, processing of sensitive data, security, for processors compliance with instructions from the controller), including rules on using processors or sub-processors and rules on Onward Transfers. Such requirements will be reflected in the Third Country Transfers Module with a focus on processors.

In reflecting those requirements in relation to processors, this Third Country Transfers Module will explicitly address the nature of the processing involved, namely, the Processing Context in the area of cloud computing. This section maps those requirements whenever they are covered by the EU Cloud CoC and, to the extent necessary, applies the aforementioned data protection principles to the specific scope of this Module.

Lawfulness and Fairness, Transparency, Security, Compliance with instructions from the controller, Rules on using processors or sub-processors

4.1.1.1 CSP shall comply with the relevant sections of the EU Cloud CoC.

The principles of Lawfulness and Fairness and Compliance with instructions from the controller, each as applicable to processors, are covered by section 5.2 of the EU Cloud CoC.

The principle of transparency, as applicable to processors, is covered particularly by Section 5.7 of the EU Cloud CoC. Where additional transparency is required in the context of Third Country Transfers, this Module includes additional provisions, such as specific information obligations in section 4.2.4 of the Third Country Transfers Module.

The principle of Security, as applicable to processors, is covered by Section 6 of the EU Cloud CoC. Where additional supplementary measures are determined necessary in the context of Third Country Transfers this additional requirement will be covered by section 4.2 "Transfer Impact Assessment" of

the Module.

The principle of Accountability, as applicable to processors, is covered particularly by Section 5.6 of the EU Cloud CoC.

The principle of Rules on using processors or sub-processors, as applicable to processors, is covered particularly by Section 5.3 of the EU Cloud CoC. Additional requirements in the context of Third Country Transfers are defined in this section of the Third Country Transfers Module.

Purpose limitation, Data minimization, Accuracy, Storage limitation, Processing of sensitive data

The EU Cloud CoC and this Module address situations where a CSP is acting as a processor. The above-mentioned principles are distinct obligations of the controller, and consequently fall outside the scope of this Module.

Onward Transfers

4.1.1.2 CSP shall proceed to an Onward Transfer only if such Onward Transfer is legitimate pursuant Chapter V GDPR.

4.1.1.3 The CSP shall make available to Customer upon request a dedicated overview if Onward Transfers apply to its sub-processors and which transfer mechanisms applies to any such Onward Transfers.

4.1.2 Notification / Communication with the Monitoring Body

4.1.2.1 CSP shall without undue delay notify the MB of any changes (e.g. due to applicable laws) with a potential impact on the Transfer Impact Assessment Transparency Document (see section 4.2.1.1) performed by the CSP by communication channel determined by the MB unless the CSP is prohibited by applicable law from notifying the MB of the relevant change.

"Changes with a potential impact" as referred to in Section 4.1.2.1 mean changes that could require re-evaluation of the Processing Context and/or different supplementary measures.

4.1.2.2 Notification under section 4.1.2.1 to the MB shall be accompanied, as far as possible, by all relevant information then in the possession of the CSP.

4.1.2.3 CSP shall establish documented procedures to ensure notification as of 4.1.2.1.

CSP should have procedures in place regarding the notification which define expected practices that CSP will follow to ensure compliance to this requirement.

4.1.2.4 If the MB has established any templates (including electronic forms) for use for notifications under section 4.1.2.1 CSPs must use those templates.

4.1.3 Suitable training on the obligations arising from the Third Country Transfers Module

4.1.3.1 The CSP shall ensure that all personnel and contractors involved in the transfer of the Customer Personal Data receives adequate training related to Third Country Transfers and Onward Transfers, as relevant for their role and job function in relation to the Cloud Services.

4.1.3.2 Additionally, to 4.1.3.1 all personnel and contractors involved in the processing of the Customer Personal Data shall receive adequate training on the obligations arising from the Third Country Transfers Module, as relevant for their role and job function in relation to the Cloud Services.

The training program should be designed to address the obligations under the Third Country Transfers Module as well as awareness of Third Country Transfers and Onward Transfers concerns. CSP personnel involved in the processing of the Customer Personal Data should receive periodic training on the obligations arising from the Third Country Transfers Module, as relevant for their job and function, in conjunction with the nature of Cloud Services concerned.

Example:

The CSP training program should make employees and contractors, role specific, aware of their responsibilities around data protection in line with the CSP's policies and procedures related to the Third Country Transfers Module.

The awareness and training program may include:

- web courses,
- lectures,
- self-study courses,
- campaigns (e.g. a data protection, or information security day),
- written communications,
- newsletters.

The program should be planned to take into consideration the roles in the organization. The program should cover security and data protection practices, policies, and procedures related to the obligations of the Third Country Transfers Module.

4.1.3.3 Such training and awareness shall be subject to timely reviews.

Training and awareness should be subject to periodic reviews, with regards to its contents, its participation, its quality and effectiveness also with regards to the means training is being provided.

4.1.4 Internal Compliance Review Programme

4.1.4.1 CSP shall implement an internal compliance review program regarding its compliance with the Third Country Transfers Module.

4.1.4.2 By the review program under section as of 4.1.4.1 CSP shall ensure and continuously monitor compliance with the Third Country Transfers Module and the EU Cloud CoC.

Such program may include an internal data protection audit (by either internal or external auditors) or other internal mechanisms for monitoring compliance with the EU Cloud CoC and Third Country Transfers Module, independently from the monitoring performed by the MB.

4.1.5 Appropriate governance

4.1.5.1 CSP shall ensure that the Data Protection Point of Contact is responsible for ensuring compliance with the data protection obligations arising from the EU Cloud CoC and the Third Country Transfers Module.

This control presupposes compliance with controls [5.9.A] and [5.9.B] of the EU Cloud CoC but also extends the competences and role of the Data Protection Point of Contact to data protection obligations arising specifically from the Third Country Transfers Module.

4.1.6 Cooperation with supervisory authorities

4.1.6.1 Cooperation with supervisory authorities is covered by section 5.11 of the EU Cloud CoC.

4.1.7 Competence of EEA courts and EEA supervisory authorities

4.1.7.1 CSP shall by means of its Cloud Service Agreement, agree to be subject to the jurisdiction of an EEA court and the competent EEA supervisory authority in any procedure aimed at ensuring compliance with the EU Cloud CoC and the Third Country Transfers Module.

E.g., the Cloud Service Agreement may specify that the jurisdiction and court shall be the jurisdiction and court of the Customer's location, or that those may be a specific jurisdiction and court as mutually agreed, or that the jurisdiction and court may be determined at the Customer's discretion.

To the extent GDPR does not provide differently, the same approach may be considered in defining the Competent Supervisory Authority ("CompSA").

4.1.8 Third-Party Beneficiary and Data Subjects Rights

4.1.8.1 The CSP shall by means of its Cloud Service Agreement, allow data subjects to enforce the CSP's obligations as third-party beneficiary rights under the Third Country Transfers Module to the extent such provisions or obligations provide direct safeguards to the data subjects. Excluding the provisions of the Cloud Service Agreement that apply specifically between the Customer and the CSP or that govern the interactions of the CSP with data protection authorities, shall not conflict with this requirement.

4.1.8.2 The CSP shall ensure that the governing law of the Cloud Service Agreement or an addendum to it (as applicable under section 4.1.8.1) allows for third-party beneficiary rights.

4.1.8.3 The CSP shall by means of its Cloud Service Agreement or an addendum to it (as applicable under section 4.1.8.1), agree that a data subject may bring legal proceedings related to

violations of third-party beneficiary rights under the Third Country Transfers Module against the CSP in the courts of the Member State where the data subject has habitual residence.

4.1.8.4 The CSP shall accept the applicability of the relevant jurisdiction and court where the requirements of section 4.1.8.3 are met.

4.1.8.5 The CSP shall not object to a data subject being represented by a not-for-profit body, organisation or association according to Article 80 (1) GDPR if the data subject expressly chooses to do so and if such representation is not prohibited by the GDPR.

4.1.8.6 The CSP acknowledges that a data subject may lodge complaints relating to the EU Cloud CoC and this Module before the CompSA.

4.1.8.7 Rights of the data subjects are specifically covered by section 5.10 "Rights of the data subject" of the EU Cloud CoC. Cloud Service Providers shall comply with controls [5.10.A], [5.11.A], [5.11.B] and [5.11.C] of the EU Cloud CoC.

4.1.9 Notification obligation in case of violation of the obligations under the Third Country Transfers Module

4.1.9.1 The CSP shall without undue delay notify the MB by the communication channels determined by the MB if the CSP becomes unable to comply with the Third Country Transfers Module. The CSP shall adequately notify the Data Exporter and the CompSA of any detected violation of the Third Country Transfers Module and any corrective measures taken by the MB in response to that violation in situations where such violation is likely to put at risk the rights and freedoms of data subjects.

Where requirement 4.1.9.1 refers to "adequately", "adequately" should comprise of both, timely manners, and communication channels. CSP shall establish documented procedures to ensure notification as of 4.1.9.1.

4.2 Transfer Impact Assessment

4.2.1 General information

4.2.1.1 For each Processing Context, the CSP shall provide the MB with the completed Transfer Impact Assessment Transparency Document (the "TIAT-Document") which is annexed as a template to the Third Country Transfers Module to be completed by Processing Context.

The TIAT-Document includes a Processing Context Assessment Template (the "PCAT") and a Legal Third Country Assessment System (the "LTCA") the elements listed in sections 4.2.2 and 4.2.3 which establishes the methodology for determining whether and/or which Supplementary Measures should apply for each Processing Context taking into account the applicable laws and practices in a Third Country. Whenever there is a substantive change to a statement provided by the CSP in the TIAT-Document in such a way that it conflicts with the obligations of the CSP under the EU Cloud CoC and

the Third Country Transfers Module, the CSP shall update the TIAT-Document and adequately notify the MB and/or the Customers promptly as provided by the Module. The updated TIAT-Document containing a substantive change shall be used by the MB as part of this module's Transfer Impact Assessment (i.e., the updated TIAT-Document may be used for Catalogue updates).

Where the requirement refers to "adequately", "adequately" must consider both the timely manner and the appropriate channels of communication where it is reasonable to expect that the Customer and the MB will be effectively informed.

4.2.2 Processing Context Assessment

The Processing Context Assessment Template or PCAT standardizes the information related to the impact and security implication of a Third Country Transfer and Onward Transfer.

The Module shall not re-allocate the obligations under GDPR, i.e., the Module acknowledges that a transfer impact assessment must be performed by the controller. Nonetheless, against the background of highly standardized Cloud Services, the controller may require significant support from the CSP in order to complete that assessment.

Thus, the Module facilitates the assessment of the Processing Context and the implemented Supplementary Measures for those Cloud Services that adhere to this Module.

4.2.2.1 The CSP shall document relevant aspects of its provision of the Cloud Service in relation to the Third Country Transfer by completing the PCAT attached as annex [x] to this Module. The impact of Customers' use of the Cloud Services, particularly those aspects of Cloud Services usage (including lack of use of available measures) that are determined by Customers, shall be outside the scope of the CSP's responsibilities under this section.

4.2.2.2 The PCAT completed by the CSP shall, at minimum, reflect the following aspects:

- the sector or industry to which the relevant CSP offers its Cloud Services;

There may be different sector-specific laws that apply to the CSP or the relevant Cloud Services. E.g., there may be specific obligations to cooperate with law enforcement agencies in the context of telecommunication services. Likewise, specific obligations to cooperate with authorities might exist in the context of banking and finance.

- if known, the type of Customer Personal Data and Data Subject categories expected to be involved in the Third Country Transfer/ nature of Customer Personal Data transferred.

Depending on the nature of the Cloud Service, the CSP may have some or limited information about the types of Customer Personal Data being transferred.

Where the CSP provides software or application as a service, the CSP may derive from the capabilities

and features of its Cloud Service which types of Customer Personal Data can be generally expected (except to the extent Customers may deliberately or negligently misuse the CSP's Cloud Service.) *Example A: A Cloud Service that provides the capabilities to make appointments with an exhaustive pre-set of fields, those fields shall determine the expected type of Customer Personal Data. Against this background, where the fields may be: Title, Sex, Name, Physical and Electronic Address of Requesting Party, Date of Requested Appointment, the type of Customer Personal Data can be concluded as Identifying Data and Contact/Address Data as well as Data in the Context of the Performance of a Contract.*

Example B: A Cloud Service that provides the capability to track and review individual drug use, the type of Customer Personal Data will certainly involve data concerning health, alongside and Contact/Address Data.

Example C: A Cloud Service provides only the option, to create – interrelated – lists and databases, or even just the mere capability to store data. Such data may be personal data, but also it may be non-personal data. The Cloud Service is designed, that there is no technical pre-determination of the expected types of Customer Personal Data. In this context, the CSP should consider requesting an identification of expected types of Customer Personal Data via the Cloud Service Agreement from the Customer. In this case, the CSP could refer to the collection of expected types of Customer Personal Data. Alternatively, the CSP may define the types of Customer Personal Data it considered during its assessment respectively which Customer Personal Data it considered to be excluded. If known by the CSP, the categories of data subjects concerned by the Third Country Transfer and if applicable Onward Transfer.

E.g., this could relate to

- minors
- employees
- accused criminals
- [TBC]

- The type and format of data processing taking place in a Third Country;
- The type and format of the data being processed in a Third Country;

E.g., this may relate to

- static or dynamic data,
- structured or non-structured data.

- A description of the Third Countries to which Customer Personal Data will be transferred in context of the Cloud Service declared adherent to the Third Country Transfers Module.
- Whether there is any Onward Transfer of Customer Personal Data within the same Third Country or Onward Transfer to another Third Country;
- The starting date of the intended Transfer Country Transfer and if applicable of the Onward Transfer;
- The duration of the intended Transfer and if applicable of the Onward Transfer.

4.2.3 Legal Third Country Assessment System (the "LTCA")

This section relates to the methodology for identifying and documenting situations such as laws or practices applicable to the Third Country Transfer and determining whether the implementation of Supplementary Measures is necessary.

The CSP must adequately support in ensuring that the protection afforded to Customer Personal Data transferred to such a Third Country is essentially equivalent to that guaranteed in the EEA by the GDPR (when read in light of the Charter of Fundamental Rights of the EU). In this respect and to assess whether the CSP may be subject to any factors such as laws or practices that may impose a risk for the processing or the rights and freedoms of the data subjects, it is necessary to first identify the jurisdictions whose laws may apply to a CSP or its provision of Cloud Services and, second, to identify whether, in relation to these jurisdictions, any factors such as specific laws or practices exist that could pose a risk to the rights and freedoms of the data subject. This assessment needs to be completed for each Processing Context. This will enable CSPs to assess whether the implementation of Supplementary Measures is required and to determine appropriate Supplementary Measures. As a result, this section deals with the methodology and documentation of these assessments.

In cases where the Customer instructs in conflict to the findings of the CSP under the LTCA, such transfers will fall outside the scope of this Module and outside the liability of the CSP.

1) Identification of Applicable Jurisdictions

4.2.3.1 The CSP shall identify the jurisdictions whose laws may apply to the CSP in relation to the Cloud Services covered by the Third Country Transfers Module and document the respective results.

For this assessment the CSP may consider different aspects relating to the processing, such as:

- the location of different establishments of the CSP
- location of the holding entity of the CSP
- locations of servers used by the CSP for the processing
- location of personnel involved in the processing
- the intended Onward Transfers

This assessment should cover both general laws and practises applicable to CSPs (e.g., tax laws) and laws and practices applicable to the specific Cloud Services (i.e. telecommunication regulations).

2) Identification of factors that exist in the Applicable Jurisdiction

4.2.3.2 The CSP shall review the jurisdictions identified pursuant to section 4.2.3.1 and document whether any factor applies that may require the CSP to conduct further evaluation to determine whether the level of data protection provided is compatible with that required by GDPR.

Factors that may require the CSP to conduct further evaluation may relate to conflict of laws (where a CSP may be prevented from complying with its obligations as a processor under the GDPR by a conflicting law in another jurisdiction), applicable laws, government practices, absence of any data protection laws or absence of the rule of law.

The CSP shall review any legislation applicable to the CSP with respect to its provision of the Cloud Service, including, but not limited to, government surveillance laws, government access rights and data retention obligations. The CSP should not only consider statutory legislation the relevant country but also court decisions and any particular practices applied by authorities even if these conflict with or exceed the statutory provisions. This will require an analysis of various aspects of the applicable legal regime to ensure relevant regulations, court decisions and governmental practices are identified.

The CSP should assess the applicable laws for any service or processing operation provided to the Customer, with the understanding that for similar Processing Contexts, only one assessment may be required.

The scope of the assessment is thus limited to the legislation, court decisions and practices relevant to the protection of the specific Customer Personal Data transferred.

The factors that may require the CSP to conduct further evaluation under this section may depend on specific circumstances that were already identified under section 4.2.2.2.

Examples of certain extraordinary factors that may require the CSP to conduct further evaluation under this section:

- Statutory rights of governmental authorities or other third parties to request access to Customer Personal Data processed by CSP;
- Statutory rights of governmental authorities or network operators to log network traffic and tap into communications (either meta data or content data);
- Statutory obligations of CSP to provide for technical means to grant governmental authorities access to Customer Personal Data processed on behalf of Customer (e.g. backdoors or similar tools);
- Statutory obligations of CSP to retain Customer Personal Data processed on behalf of Customer when this retention would contravene the Customer's instructions to the CSP with

respect to that processing;

- Statutory obligations of CSP not to use effective technical safeguards to protect Customer Personal data processed on behalf of Customers (e.g. prohibition of encryption or obligations to provide decryption keys to governmental authorities);
- Statutory obligations of CSP not to grant (foreign) data subjects access to or information about personal data stored about them or to respond to data subject rights in general (including requests concerning access by authorities);
- Statutory obligations of CSP not to provide information to Customer about governmental attempts to access Customer Personal Data processed on behalf of Customer;
- Statutory rights or evidenced practice of governmental authorities to actively hack into the CSP's systems to access Customer Personal Data processed on behalf of Customer (e.g. by trojan horses or similar attacks);
- Obligations of CSP to actively screen Customer Personal Data processed on behalf of Customer and inform authorities about certain results.

In this context, it may also be of relevance, if the legislation principally allows for a conflicting situation, but the powers provided by such legislation, de facto, have not been exercised, yet.

4.2.3.3 The CSP may consider Catalogues (see section 5.2.2) as published in the Catalogue Register (see section 5.7) in its assessments.

4.2.3.4 The CSP shall establish processes to actively monitor and review the accuracy of its findings pursuant 4.2.3.1 and 4.2.3.2.

Such process may e.g., foresee to regularly review the accuracy of its findings, or to review in case of need.

E.g., the process may govern that the CSP reviews the findings once a year and whenever it becomes aware information that could significantly impact its previous findings.

The following may be considered:

- changes relating to existing relevant regulations or practices;
- new relevant regulation or practices that are implemented in the future or;
- absence of protective legislation/lack of legislation.

4.2.3.5 If the review above identifies any factor that requires a CSP to conduct further evaluation, the CSP shall update its completed TIAT-Document accordingly.

4.2.3.6 CSP shall document the sources of information used to identify those factors.

4.2.3.7 The CSP shall only refer to sources that are objective, reliable, verifiable, and publicly available or otherwise accessible.

- Relevant: the information should refer to the specific transfer and for the CSP and its

compliance with the requirements set in EU law and this Third Country Transfers Module, and not overly general or abstract.

- Objective: the information should be supported by empirical evidence based on knowledge gained from the past, rather than assumptions about potential situations and risks.
- Reliable: the information should be reliable, i.e., where possible, original sources shall be preferred; additionally, specifically in case of information that does source from public bodies, such as courts or administrations, the reputation of the (private) source may impact its reliability. Potential biases or conflicts of interest of the sources may also impact the reliability.
- Verifiable: the information should be verifiable or contrastable with other types of information or sources.
- Publicly available or otherwise accessible information: the information should preferably be public or at least accessible to interested stakeholders under NDA. A lack of this aspect should be considered also in the context of verifiability and reliability of the information.

4.2.3.8 Catalogues as published in the Catalogue Register, shall be deemed adequate and comprehensive to the extent the identified factors for a certain Processing Context are covered.

3) Assessment of compatibility of identified factors with fundamental rights of data subjects

4.2.3.9 The CSP shall assess and document whether any factor identified pursuant to 4.2.3.2 undermines the essence of fundamental rights of data subjects.

Factors such as statutory provisions or governmental practices may undermine the essence of fundamental rights of data subjects where:

- No clear, precise and accessible rules exist for any of the identified situations:
    - Any actions by governmental authorities related to any of the identified practices must follow documented criteria which need to be clearly listed and easily understandable and accessible by data subjects.
- The practices are not considered necessary and proportionate for achieving a legitimate goal in a democratic society:
    - First, it must be ensured that any of the practices identified above serve a legitimate purpose in a democratic society, such as national security and defence, public security, prevention, investigation, detection or prosecution of criminal offences, the protection of judicial independence and judicial proceedings, the enforcement of civil law claims.
    - Second, the tool provided by applicable law or practice must be necessary and proportionate for achieving the legitimate purpose, and not excessive in regard of the envisaged purpose, e.g. where no materiality thresholds for executing a right are

provided for.

- No independent oversight mechanism exists:
    - Any actions above may only be executed under an independent oversight mechanism, e.g., subject to a court decision or at least governmental scrutiny to prevent misuse of formal investigation powers.
- Data subjects are not provided with effective remedies against any of the above practices:
    - Data subjects must be able to seek effective remedies if local authorities or third parties violate their fundamental rights or exceed their legitimate powers.

4) Determination on whether a Supplementary Measure shall be applied to the identified factor(s)

4.2.3.10 CSP shall evaluate the risks to the fundamental rights of data subjects as described in section 4.2.3.9 and determine whether any of the factors identified require the implementation of Supplementary Measures.

Supplementary Measures are likely required if:

- The minimum safeguards resulting from the principle of proportionality under EU law are not respected by the applicable law of the Third Country.

Supplementary Measures are likely not required if:

- The applicable law of the Third Country includes a balancing of interest.
- The applicable statutory right or practice respects the essence of the rights of the data subject and constitutes a necessary and proportionate measure in a democratic society to safeguard an important objective, as also recognised by the EU/EEA.
- The applicable statutory right or practice is necessary to protect the vital interests of the data subject or of another natural person.
- The applicable statutory right or practice is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings.
- International agreements are in place that guarantee mutual respect for fundamental rights and avenues for redress in the event of violations. This is provided that the agreements are implemented by their respective parties and mechanisms to enforce the defined obligations exist for the event that this is not the case.

5) Assessment, determination implementation and documentation of the adequate Supplementary Measure

4.2.3.11 Where Supplementary Measures are determined to be necessary pursuant to section 4.2.3.10, the CSP shall implement appropriate Supplementary Measures.

4.2.3.12 If an applicable Catalogue exists, the CSP may refer to the applicable Catalogue, section 4.2.3 5) (i).

4.2.3.13 When the CSP concludes that there is no Catalogue with a Processing Context that corresponds to the CSP's processing activities, or does not wish to rely on an applicable Catalogue, the CSP shall follow the procedure to individually assess and determine appropriate Supplementary Measures as outlined in section 4.2.3 5) (ii).

4.2.3.14 The CSP shall indicate in the completed TIAT Document whether its identification of Supplementary Measures relied solely on Catalogues (see section 5) (as per the procedure described in section 4.2.3 5) (i) or whether the CSP individually determined the appropriate Supplementary Measures (as per the procedure described in section 4.2.3 5) (ii).

i. Procedure regarding the assessment and determination of appropriate Supplementary Measures if one or more applicable Catalogues exist

4.2.3.15 CSP shall document which Catalogue(s) it relied on for the Cloud Services declared adherent under the Third Country Transfers Module.

4.2.3.16 CSP shall appropriately respect and reflect the findings of any Catalogues relied on by the CSP if the following provisions are met.

4.2.3.17 CSP shall assess whether any Catalogue(s) relied on by the CSP fully covers the assessment included in steps 1), 2), 3) and 4) above and therefore the Processing Context of its service(s).

4.2.3.18 If the CSP concludes that any Catalogue relied on by the CSP fully covers the assessment included in steps 1), 2), 3) and 4) and therefore the Processing Context of its service(s), CSP shall either (a) include a confirming statement in its completed TIAT and implement the appropriate Supplementary Measure as defined in the Catalogue; or (b) decide to not implement the related Supplementary Measures and document its reasons for doing so.

ii. Procedure regarding the assessment and determination of appropriate Supplementary Measures if no applicable Catalogue exists or if the CSP does not rely on an applicable Catalogue

4.2.3.19 CSP shall indicate in the completed TIAT-document its implemented Supplementary Measures.

4.2.3.20 To determine the appropriate Supplementary Measure the CSP may refer to the "Supplementary Measures Matrix" which is included in the Annex of the Module.

6) Procedure in case the CSP does not identify any adequate Supplementary Measure

4.2.3.21 Where the CSP in a Third Country received the Customer Personal Data by means of Third Country Transfer and the CSP does not, or can no longer, identify any appropriate Supplementary Measure, the CSP shall promptly inform the Customer and, allow the Customer to terminate the Cloud Services Agreement insofar as it concerns the relevant Third Country Transfers.

4.2.4 Transparency

4.2.4.1 Based on the documented assessment the following minimum information shall be made available to the Customer:

implemented and determined Supplementary Measures,4.2.3.18 and 4.2.3.19.

- whether and to what extent the assessment is based on existing Catalogues, 4.2.3.14.
- [TBC]

The availability of such information could be subject to a Non-Disclosure Agreement.

4.2.4.2 Based on the documented assessment the following minimum information as included in 4.2.4.1 shall be made publicly available:

- [TBC]

The information could be made publicly available via the CSP's website.

Such information could also be included in the Public Register alongside the listing of the adherent Cloud Service to the Module.

4.3 Situations conflicting with the obligations under the EU Cloud CoC and the Third Country Transfers Module

4.3.1.1 CSP shall assess whether factors identified in step 2) of section 4.2.3 may prevent CSP from complying with its obligations under the EU Cloud CoC or the Third Country Transfers Module.

4.3.1.2 CSP shall warrant that at the time of adhering to the Third Country Transfers Module it has no reason to believe that the laws applicable to it or the processing of Customer Personal Data in any Third Country prevent it from fulfilling its obligations under the EU Cloud CoC or the Third Country Transfers Module.

The monitoring and review process described under section 4.2.3.4 shall also entail periodic reviews to determine whether any situation will prevent the CSP from complying with the Third Country Transfers Module.

5 Independent Risk Advisory Body (IRAB)

5.1 Subject matter and principles

5.1.1.1 The IRAB shall be an independent body which co-operates with the MB, as well as with the CompSA, within the framework of this Module, to develop and update Catalogues.

Catalogues are intended to help CSPs and their Customers determine appropriate Supplementary Measures in relation to a specific Processing Context.

5.2 Responsibilities

5.2.1 Collection of Information

5.2.1.1 The IRAB shall enable the MB to communicate information to the IRAB that the MB considers relevant in the context of the establishment of Catalogues.

5.2.1.2 The IRAB shall acknowledge receipt to the MB of the communication.

5.2.1.3 The IRAB shall document the information it receives from the MB.

5.2.1.4 The IRAB shall evaluate the information it receives from the MB in order to a) define relevant Processing Contexts and b) determine adequate Supplementary Measures per Processing Context.

5.2.1.5 The IRAB shall attribute a unique identifier per Processing Context. This unique identifier shall be used in subsequent documents by the IRAB.

5.2.1.6 The IRAB shall continuously and systematically analyse whether any additional information it receives from the MB relates to information previously received from the MB, and consider whether, in light of any such additional information, new Processing Contexts should be defined, or any existing Processing Contexts, or related Catalogues should be updated.

5.2.2 Establishment of Catalogues

5.2.2.1 The IRAB shall develop and publish Catalogues.

5.2.2.2 In the developing process of the Catalogues the IRAB may consult the General Assembly regarding particular Supplementary Measures applicable in a specific Processing Context. However, the IRAB is not obliged to incorporate the feedback received from the General Assembly through such consultation in the final Catalogues.

5.2.2.3 Each Catalogue shall enable a CSP to easily assess whether the Catalogue applies to its Cloud Service.

5.2.3 Continuous Review and Update of Catalogues

5.2.3.1 The IRAB shall continuously review its published Catalogues.

5.2.3.2 Where necessary, the IRAB shall update existing Catalogues.

5.2.3.3 If the IRAB receives any information that conflicts with an existing Catalogue, the IRAB shall, in due time, evaluate the situation and take appropriate actions as defined in IRAB's operating procedures such as adapting the Catalogue or suspending the application of the Catalogue.

5.2.4 Release of a new Catalogue or updated version of a Catalogue

5.2.4.1 The IRAB shall inform the MB about any updated Catalogues.

5.2.4.2 The IRAB shall publish its updated Catalogues as outlined in section 5.2.2 in a register (the "Catalogue Register").

5.3 Interaction with Competent Supervisory Authority

5.3.1.1 The IRAB shall ensure that any new or updated version of any Catalogue has been communicated to the CompSA.

5.3.1.2 The CompSA shall be entitled to provide feedback on any communicated Catalogue.

5.3.1.3 The IRAB shall allow the CompSA a reasonable period within which to provide any feedback; such period shall not be less than ninety (90) calendar days.

5.3.1.4 If the CompSA provides adverse feedback on any submitted Catalogue, e.g., where the CompSA requests changes, the IRAB shall evaluate that feedback and take any appropriate actions (which may include updating the Catalogue to address any concerns of the CompSA). The IRAB may also conclude that no actions are necessary, for example where the CompSA does not provide reasons for its feedback or where any concerns of the CompSA can be addressed otherwise.

5.3.1.5 Following evaluation by the IRAB of any adverse feedback from the CompSA, the IRAB shall inform the CompSA of the IRAB's conclusions (and submit to the CompSA any updated version of the Catalogue created to address its concerns).

5.3.1.6 In response to the IRAB's conclusions (including any updated version of the Catalogue submitted by the IRAB to the CompSA), the CompSA may either repeat its previous feedback, where it does not consider its concerns to have been adequately addressed by the IRAB, or comment initially on other elements of any updated Catalogue.

5.3.1.7 If the CompSA provides feedback pursuant to section 5.3.1.6, the process as defined in sections 5.3.1.4 to 5.3.1.6 shall apply accordingly.

5.4 Appointment, Independence, and Expertise

5.4.1.1 The IRAB can either be established as a body within the EU Cloud CoC or outsourced to an external entity.

5.4.1.2 If the IRAB is being outsourced to an external entity, that entity shall be appointed by the General Assembly of the EU Cloud CoC.

5.4.1.3 There shall be only one IRAB at a time for this Module.

5.4.1.4 The General Assembly shall only appoint an external entity that meets the following requirements:

a. solid expertise relating to the Cloud Computing sector
b. solid expertise relating to the GDPR
c. transparent and fair procedures and performance of its activities
d. solid expertise in the subject matter of third country transfers
e. [TBC]

5.4.1.5 The General Assembly shall establish documented procedures ensuring that the performance of the IRAB with regard to compliance with its obligations as outlined in section 5 is constantly monitored by the General Assembly to the extent possible.

5.4.1.6 The General Assembly shall withdraw or suspend the appointment of the IRAB in case of factual indications that the IRAB no longer meets the requirements as defined in this Module, particularly in case the monitoring of the IRAB according to section 5.4.1.5 has revealed a violation of obligation by the IRAB.

5.4.1.7 The General Assembly shall inform the CompSA about the appointment of an external entity to represent the IRAB or withdrawal and any changes related to that entity.

5.4.1.8 The CompSA shall be entitled to request from the General Assembly any relevant and information related to the appointment or withdrawal of the appointment.

5.4.1.9 The CompSA shall be entitled to communicate to the General Assembly any feedback regarding the IRAB and related decisions by the General Assembly.

5.4.1.10 The General Assembly shall evaluate any feedback it receives from the CompSA and take any appropriate actions such as adapting the decisions under this section; the General Assembly may also conclude that no actions are necessary, for example where the CompSA does not provide reasons for its feedback or where any concerns of the CompSA can be addressed otherwise.

5.4.1.11 Following evaluation by the General Assembly of any feedback from the CompSA, the General Assembly shall inform the CompSA of the General Assembly's conclusions.

5.5 Liability and financing

5.5.1.1 The IRAB shall be awarded adequate resources, including financial and human resources, by the General Assembly, sufficient to ensure the IRAB's independence and the due performance of its duties.

5.5.1.2 The IRAB must not be held responsible for any reliance by CSPs on a published Catalogue or implementation of any measure included therein (including any damages, penalties or other losses suffered or incurred as a result of such reliance).

5.6 Composition of the IRAB

5.6.1.1 The IRAB shall be composed of experts who have proven expertise in the field of cloud computing and/or data protection, particularly with regard to international data transfers.

5.6.1.2 The IRAB shall ensure that the experts involved in its decision making, and are free from undue conflicts of interest. The experts shall not be involved in the monitoring of the Module, i.e. the processing of declarations of adherence or related complaints.

5.6.1.3 The IRAB may allocate its duties across different units, allowing for an efficient performance, e.g., the IRAB may create one unit to perform administrative functions and another unit to perform functions integral to the IRAB's responsibilities relating to protection of transferred data.

5.6.1.4 Representatives of the General Assembly and the MB may be entitled to participate in the meetings of the IRAB as guests, provided such participation does not conflict with the due performance of the IRAB's responsibilities.

5.7 Catalogue Register

5.7.1.1 The IRAB shall maintain a digital register of its published Catalogues.

5.7.1.2 The Catalogue Register shall enable relevant stakeholders to easily access existing Catalogues.

Relevant stakeholders should include – at a minimum – the MB and CSPs declaring adherence to the Module.

5.7.1.3 The Catalogue Register shall enable relevant stakeholders to easily determine, whether a Catalogue exists for a specific Processing Context.

5.7.1.4 The Catalogue Register shall identify whether the CompSA provided feedback on the existing Catalogues.

5.7.1.5 The Catalogue Register shall explicitly indicate if any adverse feedback from the CompSA was not resolved by the IRAB prior to publication. Where there is no such indication in the register for any Catalogue, relevant stakeholders shall be entitled to rely in good faith on there being no unresolved adverse feedback relating to the relevant Catalogue. Accordingly, stakeholders may assume that the CompSA did not identify aspects of such Catalogue that would conflict with legitimate Third Country Transfers given the Processing Context if they implemented the Supplementary Measures of the Catalogue and thus may be deemed adequately protected.

6 Monitoring and Compliance

6.1 Introduction

This section governs all provisions related to the appointment of the MB, adherence of Cloud Services to the Third Country Transfers Module, compliance of adherent Cloud Services, and the monitoring of and complaints' handling under the Third Country Transfers Module.

6.2 The Monitoring Body

This section is governed by Section 7.2 of the EU Cloud CoC.

6.3 Conditions of Adherence

CSPs that consider one or more of their Cloud Services, already verified under the EU Cloud CoC, to meet the requirements set out in the Third Country Transfers Module, can submit a declaration of adherence for any or all of those Cloud Services to the MB: (a) if those Cloud Services have already been verified under the EU Cloud CoC and if the transfer falls with the scope of this Module. In this case, the relevant Cloud Services shall be considered adherent to this Module once they pass the assessment for this Module; or (b) if those Cloud Services have not yet been verified under the EU Cloud CoC and if the CSP's declaration of adherence by those Cloud Services to this Module is accompanied by a declaration of adherence by those Cloud Services to the EU Cloud CoC. In this case, Cloud Service shall only be considered adherent to this Module and the EU Cloud CoC once they pass the assessments for both this Module and the EU Cloud CoC.

By submitting a declaration of adherence of Cloud Services to the Third Country Transfers Module, the CSP commits to comply with the requirements of the Third Country Transfers Module for any Cloud Services covered by its declaration. Any Cloud Services declared adherent to the Third Country Transfers Module must comply with all requirements of the Module.

Verified adherence of Cloud Services to the Third Country Transfers Module does not absolve any CSP from having to comply with the GDPR, and/or applicable EU Member State data protection law, nor does it protect CSPs from possible interventions or actions by supervisory authorities in the course of their supervision and enforcement activities with regards to the adherent Cloud Services. GDPR and applicable Member State laws will always prevail over the Third Country Transfers Module. Cloud Services declared adherent will undergo rigorous scrutiny by the MB. Without prejudice to sanctions from competent authorities as foreseen in case of breaches of the GDPR and/or other legal acts, CSPs, which fail to meet the requirements of the Third Country Transfers Module, will be subject to the enforcement mechanisms as set out in this Section of the module.

6.4 Procedure to declare a Cloud Service adherent

CSPs submit their declaration of adherence to the MB following the procedures provided by the Third Country Transfers Module and by the MB. The procedures published by the MB may determine that a submission of a declaration of adherence shall be received only by utilizing distinct templates or online forms. The MB shall provide to the CSP any template that must be used by the CSP to achieve adherence with the Third Country Transfers Module.

Upon request by the MB, the CSP shall provide information relevant for the declaration of adherence in an up-to-date and accurate manner. A CSP shall notify the MB promptly whenever information provided within the declaration of adherence becomes outdated or inaccurate, regardless of its reason. Providing outdated or false information could amount to an infringement of the Third Country Transfers Module. The lack of notification shall be treated as providing outdated or inaccurate information.

The MB shall review the declaration of adherence in due time and update the Public Register accordingly.

CSP shall renew its declaration every year.

6.5 Assessing compliance with the Third Country Transfers Module

6.5.1 Controls

To ensure that the MB can verify that requirements of the Third Country Transfers Module are met by the Cloud Services declared adherent, requirements of this Module are reflected by Controls. Each Control is given a unique identifier (“Control-ID”) following this pattern: section, subsection. sub subsection, number e.g. 6.5.3.1.

6.5.2 Ambiguous Requirements

If and to the extent the Third Country Transfers Module or a Control leaves room for interpretation, e.g. where it requires reasonable assistance, the MB shall provide the final conclusive decision on whether the Third Country Transfers Module’s requirement is being complied with. The MB shall consider any notion provided by the Third Country Transfers Module (e.g., the background explanation and context, guidance implementation, Catalogues and Supplementary Measures Matrix).

6.5.3 Options available to CSPs

6.5.3.1 CSPs declaring adherence to the Third Country Transfers Module may do so with or without use of Catalogues, to the extent Catalogues exist.

6.5.3.2 The MB shall assess whether CSP followed the process defined by this Module to assess and determine appropriate Supplementary Measures.

6.5.3.3 The MB shall have the power where necessary, for example, in case of doubt, to assess whether the Supplementary Measures are implemented.

6.5.3.4 Unless the MB has reasons to believe a CSP does not conform with the Module or any of its concluded measures, the assessment by the MB shall be limited to assessment of CSP's policies and procedures ensuring conformity with the Module.

6.5.4 Ad hoc assessment of the TIAT-Document following a change

6.5.4.1 When the MB is notified by CSP about any changes of applicable laws, practices or any other elements that may have an impact whatsoever on the transfer impact assessment as outlined in section 4.1.2.1, and receives the updated TIAT-Document, the MB may perform an ad hoc assessment of the TIAT-Document.

6.6 Compliance mark

[A dedicated compliance mark will be designed to communicate compliance with this Module.]

6.7 Monitoring and enforcement

Section 7.7 of the EU Cloud CoC shall apply mutatis mutandis to the Third Country Transfers Module.

6.8 Complaint Handling and procedure

Section 7.8 of the EU Cloud CoC shall apply mutatis mutandis to the Third Country Transfers Module.

6.9 Sanctions and remedies

Section 7.9 of the EU Cloud CoC shall apply mutatis mutandis to the Third Country Transfers Module. As within the EU Cloud CoC, if a Cloud Service declared adherent to the Third Country Transfers Module and the Third Country Transfer is non-compliant with any requirement of the Third Country Transfers Module, the applicable CSP shall be subject to appropriate sanctions and remedies. As a result, remedies include the powers of the MB to require the CSP to remediate the violation of the Third Country Transfers Module.

6.10 Governance

The Third Country Transfers Module is governed by the EU Cloud Code of Conduct Internal Governance Code which is binding and constitutes an essential element of the Module. The EU Cloud Code of Conduct Internal Governance Code is available on the EU Cloud CoC website.

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.