EU Cloud Code of Conduct

EU CLOUD COC

Controls Catalogue – template for DoA

EU Data Protection Code of Conduct for Cloud Service Providers

Related Code Version:	2.12
Template Publication Date:	September 2026
Website:	https://eucoc.cloud

1 Introduction

1.1 Background

The EU Cloud COC provides dedicated controls that must be met by each Cloud Service. Therefore, please declare per each control, how the declared Cloud Service (family) complies with the respective control. Please keep in mind, also, that you will have to comply with all provisions of the Code that are using "must", "shall", "have to", no matter whether they are mentioned in the Code itself, translated into dedicated Control or used in the Control Guidance. The Monitoring Body may refer to such provisions as well, especially to the extent the Monitoring Body considers your responses to the Controls not covering such remaining mandatory provisions, yet.

1.2 Expectations of the Monitoring Body (Examples)

As the implemented measures may materially differ between different Cloud Services and Cloud Service Providers (CSPs), there is no specific template how to do so. However, please take into account the following examples and general remarks, when completing the template:

- *[5.1.C] Responsibilities of the CSP and the Customer with respect to security measures under GDPR shall be defined, documented, and assigned in the Cloud Services Agreement.*

Whenever there is requirement that is as precise as within this control, please give exact references. In 5.1.C, e.g. give precise reference which provision(s) in your Cloud Service Agreement correlate with the control, please. It will not suffice to generally refer to your Cloud Service Agreement, as it is not up to the Monitoring Body to research which provisions might be considered relevant or interferent for the control.

- *[5.2.B] CSP shall establish documented procedures, that enables Customer to access relevant information to comply with its obligations and duties under GDPR.*

Whenever there is a requirement to implement procedures, please provide a short description of the procedure being in place. Where documentation is required, please indicate where and how the procedure is documented. It will not suffice to only refer to any documentation without describing the principles and steps of the procedure. Nor will it suffice – where documentation is required – to only describe the procedure without referencing the documentation (e.g. file name, file version, storage). Please also keep in mind, that a documented procedure or policy is expected to indicate its version, department / personnel responsible for maintaining / signing-off the procedure / policy, and in which cases the procedure / policy is applicable.

- *Referencing international certificates and audit reports*

Most likely, in Section 6 you will underpin your declaration with international certificates and audit reports. Please reference the relevant sections and scope of the respective reports / certificates for each control. It will not suffice to only note "ISO XXXXX" or "SOCXX" certified. In case a Cloud Service complies with multiple certifications / audits keep in mind, that only those being referenced in this template will be taken into account by the Monitoring Body when assessing a Cloud Service's compliance with the EU Cloud CoC.

- *Referencing nature of processing*

To the extent your responses refer to the "nature of processing", please indicate why the nature of processing results into limitations of the implementation of this control.

1.3 Guidance on responding to Control Specifications and Supporting Questions in the Declaration section

The Declaration section contains questions that elaborates on and refines the Control requirements and Control Guidance. These questions neither replace nor amend the Control requirements and Control Guidance, nor do they introduce any additional context. They are provided to break down the requirements into a more granular format, enabling CSPs to address individual Control requirements more clearly, particularly where a Control encompasses multiple dimensions and/or requirements. Please find below the instructions on how to read and complete the Declaration section, using Controls 5.2.D and 5.7.A as examples.

As Control 5.2.D addresses multiple dimensions, it is reflected through Control Specifications (e.g. 5.2.D.1 and 5.2.D.1.1). Control Specifications are presented as questions in bold and require a Yes / No response.

The response shall be provided by deleting the option that is not applicable, as illustrated in the table below.

[5.2.D] CSP shall process Customer Personal Data according to Customer's Instructions. The scope of Customer's Instructions for the processing of Customer Personal Data shall be defined by the Cloud Services Agreement.	5.2.D.1. **Does the Cloud Services Agreement determine the scope of the Customers instructions for the processing of the Customers Personal Data?** Yes
	...
	5.2.D.1.1 **Does the CSP have procedures in place to ensure that Customer Personal Data is processed according to Customers documented instructions?** Yes
	...

1.3.1 Level 1 – Control Specifications

At Level 1, Control Specifications always include the Control identifier (e.g. 5.2.D) followed by the number of the specific question in bold (e.g. 5.2.D.1). Where more than one Control Specification applies within the same Control, they are identified by extending the numbering (e.g. 5.2.D.1.1, 5.2.D.1.2, and so forth). All Level 1 Control Specifications shall be responded, unless otherwise indicated.

However, Control Specifications may be presented as alternative questions, this is indicated by separate numbering approach (e.g. 5.7.A.1 and 5.7.A.2, as applicable to Control 5.7.A). In such cases, the Control Specifications shall be read in the order of appearance and response shall be only provided to the applicable Control Specification (e.g. either 5.7.A.1 **or** 5.7.A.2). Please see the table below for reference.

[5.7.A] CSP shall establish documented procedures to assist the Customer for fulfilling data subject access requests.	5.7.A.1. **Does the CSP provide the Customer with the ability to address data subjects access requests from a technical perspective (i.e., through self-service functionalities)?** No
	...
	5.7.A.2. **If no self-service functionalities are provided, does the CSP pro-vide reasonable assistance to the Customer in addressing data subjects access requests?** Yes
	...

1.3.2 Level 2 – Supporting Questions

At Level 2, Control Specifications are followed by open-ended questions, marked by lowercase letters (e.g. *a., b.*). These questions are intended to support the Yes/No response by providing further direction to CSPs on the information expected to be provided in a response. All Level 2 questions shall be answered, and responses shall be provided in the row immediately following the respective question.

Where a response is provided only under one alternative Control Specification (e.g. either 5.7.A.1 **or** 5.7.A.2), responses are required solely for the selected Control Specification and all its underlying Level 2 supporting questions.

Please see the table below for reference.

[5.7.A] CSP shall establish documented procedures to assist the Customer for fulfilling data subject access requests.	5.7.A.1. **Does the CSP provide the Customer with the ability to address data subjects access requests from a technical perspective (i.e., through self-service functionalities)?** Yes
	a. Which documentation is provided to the Customer to support them in this regard?

	Response to be provided here.
	b. Which additional support is provided to the Customer, to the extent the Customer requires additional information (beyond the documentation in a)?
	Response to be provided here.

1.4 Keep in mind the consequences if expectations are not met!

For the avoidance of doubt: if your responses are not convincing, as they may either lack material level of detail, the reference may be imprecise or lack references to other provisions that may be applicable as well, or you provide details regarding your procedures but the reference to your documents is missing, the Monitoring Body will consider your response as incomplete / inconsistent. Especially if you are passing an initial assessment, this will, in best case, only delay the verification process; in worst case scenarios, especially if the Monitoring Body provided you with chances to enhance your provided response by requesting follow-up responses, the Monitoring Body will consider your repeated insufficient responses as not being capable to convince the Monitoring Body of your compliance anymore; hence it will stop the verification and consider your declared services as non-compliant with the Code – at least for the time being. This will not hinder you to start a new verification process as soon as you have better prepared yourself and thus being able to convincingly respond to the Monitoring Bodies requests.

1.5 Your To Do

Taking into account the aforementioned, please fill in this template to enable the Monitoring Body to perform its assessment.

2 Section 5

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.1.A] A Cloud Services Agreement shall be in place between the CSP and the Customer, incorporating the data protection obligations under GDPR as a minimum.	*Controls in this section cover two dimensions, current (existing) customers and future customers. Please keep this in mind when responding. Please, also note, that in case of an international CSP, it is at a minimum expected that Customers are indicated the possibility and necessity to sign any GDPR related contractual exhibits, addenda or similar, where GDPR related provisions are not covered by the general terms and conditions already.*	
	5.1.A.1. **Is a Cloud Services Agreement in place between the CSP and the Customer?** Yes / No	
	a. Please provide a copy of the Cloud Services Agreement in place.	
	5.1.A.1.1 **Does the Cloud Services Agreement incorporate at least the same level of rights and protections afforded by the GDPR?** Yes / No	
	a. Please explain how.	
[5.1.B] A Cloud Services Agreement shall be in place providing substantially similar levels but no less protective data protection obligations as provided for by this Code.	*Please note that this Control goes beyond GDPR.*	
	5.1.B.1. **Does the CSP confirm that the Cloud Services Agreement provides data protection obligations that are at least as protective as those outlined in this Code?** Yes / No	
	a. Please explain further.	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.1.C] Responsibilities of the CSP and the Customer with respect to security measures under GDPR shall be defined, documented, and assigned in the Cloud Services Agreement.	5.1.C.1. **Does the Cloud Service Agreement define the roles and responsibilities of CSP and Customer with respect to security measures?** Yes / No	
	a. Please explain the approach with regards to the distribution of roles and responsibilities.	
[5.1.D] CSP shall have established documented procedures to ensure that its personnel is aware of the adherence to and the requirements of the Code to adequately deal with related Customer inquiries.	*In case of an **Initial Assessment**, it is not expected that any training or other means of awareness raising has already taken place. In this case, please ensure to indicate your intended measures your Cloud Service will be verified compliant with the Code.* *In case of a **Renewal**, please indicate your means of awareness raising. Personnel that are dealing with Customer inquiries shall be aware of the EU Cloud CoC and your adherence, to allow your personnel to respond accordingly.*	
	5.1.D.1. **Does the CSP provide training or other mechanisms to ensure its personnel is aware of the adherence to the Code?** Yes / No	
	a. Please provide details regarding such trainings / awareness raising mechanisms, as pertaining to the CSP's adherence to the Code.	
	5.1.D.1.1 **Does the CSP have procedures in place to address individual inquiries, complaints and disputes around non-compliance to the Code?** Yes / No	
	a. Which procedure?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	b. *Please provide a high level summary of the procedure, as pertaining to this Control.*	
[5.1.E] CSP shall transparently communicate to Customers its adherence to the Code, at least as laid down in Section 7.6.4 of this Code.	*In case of an **Initial Assessment**, it is not expected that any communication of adherence already takes place. However, it is expected to indicate where and how such required communication shall be implemented once your Cloud Service will be verified compliant with the Code.* *In case of a **Renewal**, please indicate by means of URL or screenshot where and how the required communication takes place.*	
	5.1.E.1. **Does the CSP transparently communicate its adherence to the Code?** Yes / No	
	a. Is such communication in line with section 7.6.4 of the Code? Yes / No	
	b. Where does the communication take place?	
	c. How does the communication take place?	
	d. Please provide the URL or screenshot of such communication.	
	5.1.E.1.1. **Does the CSP provide the Customer with transparent and accessible information on how to file a complaint?** Yes / No	
	a. Please provide details.	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.1.F] The Cloud Services Agreement shall determine the terms under which the CSP shall process Customer Personal Data on behalf of the Customer.	5.1.F.1. **Does the Cloud Services Agreement determine the personal data processing activities conducted by the CSP on behalf of the Customer?** Yes / No *a. Please provide the data processing activities taking into account the security, confidentiality, processing integrity, availability and data protection of the Customer Personal Data.*	
[5.1.G] The Cloud Services Agreement shall determine the terms under which the CSP can engage subprocessors in the delivery of the Cloud Service to the Customer.	5.1.G.1. **Does the Cloud Services Agreement define the terms related to the use of subprocessors by the CSP?** Yes / No *a. Please indicate the terms.*	
[5.1.H] The Cloud Services Agreement shall define the processing activities in relation to Customer Personal Data engaged in by the CSP and any sub-processors.	5.1.H.1. **Does the Cloud Services Agreement document the terms related to the processing activities by the CSP and any other third-party engaged by the CSP or Customer?** Yes / No *a. Please indicate the terms.*	
[5.2.A] CSP shall assist Customer to comply with its obligations under Article 28 GDPR to the extent the CSP is involved in the	5.2.A.1. **Does the Cloud Services Agreement define the roles and responsibilities of CSP and Customer with respect to the processing of personal information?** Yes / No	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
processing of Customer Personal Data taking into account the nature of the processing and the information available to the CSP.	*a. Please specify the respective roles.*	
	5.2.A.1.1 **To the extent the CSP is involved in processing Customer Personal Data, does the Cloud Services Agreement include the CSP's obligation to assist the Customer in complying with GDPR?** Yes / No	
	a. Please provide details regarding such assistance.	
[5.2.B] CSP shall establish documented procedures, that enables Customer to access relevant information to comply with its obligations and duties under GDPR.	5.2.B.1. **Does the CSP have procedures in place to ensure that necessary information relating to the processing of Customers' Personal Data is made available to the Customer?** Yes / No	
	a. Which procedure?	
	b. Please provide details on which type of information is made available to the Customer (e.g. third party attestations, options to audit, communication channels...etc.).	
[5.2.C] CSP shall communicate mechanisms to the Customer how to access the information of 5.2.B.	5.2.C.1. **Does the CSP provide mechanisms to the Customer that allow access to the information referred in 5.2.B?** Yes / No	
	a. Which mechanisms (e.g., Customer Portal, Customer communication channels, published resources etc.)?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	b. Please provide details on how Customer is made aware of such mechanisms.	
[5.2.D] CSP shall process Customer Personal Data according to Customer's Instructions. The scope of Customer's Instructions for the processing of Customer Personal Data shall be defined by the Cloud Services Agreement.	5.2.D.1. **Does the Cloud Services Agreement determine the scope of the Customers instructions for the processing of the Customers Personal Data?** Yes / No	
	a. Please indicate how.	
	5.2.D.1.1 **Does the CSP have procedures in place to ensure that Customer Personal Data is processed according to Customers documented instructions?** Yes / No	
	a. Which procedure?	
	b. Please provide details on the aspects covered by such procedures (e.g. format of acceptable instructions, confirmation of Customer interactions and verification, records of completion and actions taken etc.).	
[5.2.E] CSP shall establish operational mechanisms to maintain data retention policies and schedules regarding Customer Personal Data.	*Control [5.2.E] was intended for Services that are designed as a pipeline, i.e., where the level of automation is so high, that Customers input data that is being computed to get the results, but where there is no further instruction in regards of retaining such data. This might refer to scenarios where the Cloud Service will regularly delete its caches either periodically, or by new processing requests. Alternatively, this may refer to scenarios, where the processing result is being available to Customers – e.g., to be downloaded – for a distinct period.*	
	5.2.E.1. **Does the CSP have operational mechanisms and schedules in place to maintain data retention policies and schedules regarding Customer Personal Data?** Yes / No	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	a. Which mechanisms and schedules?	
	b. Please provide details on such mechanisms and schedules.	
[5.2.F] CSP shall train its personnel on such retention policies and schedules regarding Customer Personal Data and shall undertake oversight and monitoring to ensure that such schedules are followed.	*Please keep in mind the Control Guidance. Extent of applicability of this control depends on your response to [5.2.E].*	
	5.2.F.1. **If general retention schedules are provided, does the CSP train its personnel on such retention policies and schedules?** Yes / No	
	a. Please provide details regarding such training.	
	5.2.F.1.1 **Does the CSP establish appropriate monitoring to ensure that such schedules are followed?** Yes / No	
	a. Please explain further.	
[5.2.G] CSP shall communicate its standard retention policies and schedules regarding Customer Personal Data to its Customers.	*Please keep in mind the Control Guidance. Extent of applicability of this control depends on your response to [5.2.E].*	
	5.2.G.1. **Does the CSP have a mechanism in place to communicate its standard retention policies and schedules to its Customers?** Yes / No	
	a. Which mechanism?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.3.A] CSP shall obtain written authorization of the Customer prior to the processing of Customer Personal Data when engaging subprocessors.	5.3.A.1. **Does the CSP have a mechanism in place to ensure that written authorization of the Customer is in place, prior to engaging subprocessors?** Yes / No	
	a. Please indicate which mechanism is used to obtain authorization from the Customer (e.g., authorization per Customer or a general pre-authorization).	
[5.3.B] In the case of the rejection of the subprocessor by the Customer, CSP must follow the agreed upon procedures in the Cloud Service Agreement and provide alternative options such as change of subprocessor or let the Customer exercise termination rights.	5.3.B.1. **If a Customer rejects a subprocessor, does the CSP follow the agreed upon procedures in the Cloud Services Agreement?** Yes / No	
	a. Which procedures?	
	5.3.B.1.1 **Does the CSP provide alternative options (such as a change of subprocessor or an option to exercise termination rights)?** Yes / No	
	a. Please indicate which alternative options are provided to the Customer.	
[5.3.C] CSP shall establish documented procedures that ensure that it only engages subprocessors that can provide sufficient guarantees of compliance with the GDPR.	5.3.C.1. **Does the CSP have procedures in place to evaluate any subprocessors which the CSP will engage in Customer Personal Data processing activities?** Yes / No	
	a. Which procedure?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	b. Please provide details on the aspects of such evaluation (e.g. the nature of the personal data processing activities of the subprocessor, the geographical reach of the subprocessor etc.).	
	c. To the extent such procedure is part of supplier's onboarding, please explain how the CSP verifies that subprocessors can provide sufficient guarantees of compliance with the GDPR.	
	d. To the extent a risk-based approach is used (e.g., high, medium or low risk subprocessors), please confirm the minimum threshold for the engagement of subprocessors.	
[5.3.D] Documented procedures shall be implemented to flow down the same data protection obligations and appropriate Technical and Organizational Measures which are no less protective than those provided by the CSP throughout the full subprocessing chain.	*Please keep in mind that this control requires to flow-down measures, that are no less protective than those provided by the CSP. Hence, a general reference to "GDPR compliance" of subprocessors will not suffice.*	
	5.3.D.1. **Does the CSP have procedures in place to ensure that the same data protection obligations as set out in the Cloud Services Agreement with the Customer and that the subprocessor has technical and organisational controls in place that are no less protective than those of the CSP?** Yes / No	
	a. Which procedure?	
	b. Please provide details on such procedures.	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	c. Please explain how this is ensured throughout the full subprocessing chain.	
[5.3.E] Before Customer formally enters the Cloud Service Agreement, CSP shall make available to Customer – publicly or subject to a non-disclosure agreement – at least general information communicating existing subprocessors and related jurisdictions applicable to the processing of Customer Personal Data.	*Please note: given the Guidance to this Control, an indication of each subprocessor's name, legal form and location may be reasonable, as it allows Customers to determine any applicable jurisdictions.*	
	5.3.E.1. **Does the CSP make available to the Customer general information on the existing subprocessors and related jurisdictions?** Yes / No	
	a. Please provide details on the information that is made available to the Customer.	
	b. Please provide details on how such information is made available to the Customer.	
[5.3.F] CSP shall put in place a mechanism whereby the Customer shall be notified of any changes concerning an addition or a replacement of a subprocessor engaged by the CSP based on a general authorization by the Customer.	5.3.F.1. **Does the CSP have a mechanism in place to notify the Customer of changes in its subprocessors ?** Yes / No	
	a. Which mechanism (e.g., website, email, Customer Portal, etc.)?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.3.G] Notwithstanding the applicability of [5.3.F], CSP shall put in place a mechanism whereby the Customer shall be notified of any changes concerning applicable jurisdictions to a subprocessor engaged by the CSP where the CSP agreed upon processing Customer Personal Data in the scope of certain jurisdictions only and has been granted prior general authorization by the Customer to do so.	*Please note: In this Control "applicable jurisdiction" must be understood broadly. First, given the Guidance, this Control only applies if a limited set of applicable jurisdictions is guaranteed. Second, the term applicability is understood in the sense of any aspects that may influence the applicability. E.g., if a subprocessor's (main) shareholders will change, this might affect the applicability of jurisdictions to such subprocessor. Consequently, given a guaranteed limitation of applicable jurisdictions, this Control would require a notification in such scenarios. In other words: this Control does not necessarily require a change of location of subprocessors' head-quarters or places of processing.* *Please also note that a "**not applicable**" is sufficient if this is not applicable to the CSP.*	
	5.3.G.1 **Does the CSP agree upon processing Customer Personal Data in the scope of specific jurisdictions only and has been granted prior general authorization by the Customer to do so?** Yes / No	
	a. If yes, which notification mechanism has been put in place by the CSP to notify the Customer of any changes of the applicable jurisdictions to a subprocessor engaged by the CSP (e.g., website, email, Customer Portal, etc.)?	
Please note that Controls in this section cover two dimensions: a CSP a potential receiver outside the EEA and a CSP transferring personal data to sub-processors – where applicable – who may process data outside the EEA. Please keep this in mind when responding.		
[5.4.A] CSP shall utilize the appropriate mechanisms permitted by Chapter V GDPR and/or any special provisions of such mechanisms when transferring Customer Personal Data. Protective measures as provided by such mechanisms must be in place to ensure the security of data transfer.	5.4.A.1. **Does the CSP have mechanisms in place to ensure that protective controls are in place to ensure the security of data transfer when transferring Customer Personal Data?** Yes / No	
	a. Please explain further.	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.4.B] CSP shall only transfer Customer Personal Data to a third country outside the EEA if and so far, as agreed upon in the Cloud Service Agreement.	5.4.B.1. **Does the CSP have procedures in place to ensure that Customer Personal Data to third countries outside the EEA is only transferred to the extent and modalities provided by the Cloud Service Agreement?** Yes / No	
	a. Please explain further.	
[5.4.C] CSP shall ensure that transfers of Customer Personal Data to a third country outside the EEA by the CSP on behalf of the Customer, and as agreed with the Customer, meet the requirements of GDPR, Chapter V.	5.4.C.1. **Does the CSP have procedures in place to ensure that transfers of data to a third country outside the EEA meet the requirements of Chapter V GDPR?** Yes / No	
	a. Which safeguards are relied upon for the transfers from Customers to the CSP?	
	b. Which safeguards are relied upon for the transfers from the CSP to the subprocessors?	
	c. To the extent more than one safeguard is relied upon, please confirm whether there is an overarching safeguard that applies by default.	
[5.4.D] CSP shall continue to assess and monitor whether a country that is the destination of a data transfer under the Cloud Service Agreement is subject to an adequacy decision of the Commission.	*Please note that this Control might not be applicable if Adequacy Decisions are not relied upon for transfers of Customer Personal Data.*	
	5.4.D.1. **Does the CSP have procedures in place to determine and monitor if the destination of a data transfer is subject to an adequacy decision?** Yes / No	
	a. Which procedure?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	b. Please explain further.	
[5.4.E] For data transfers with a destination that is outside the EEA the CSP shall document the specific safeguards under Chapter V GDPR a transfer is based upon and shall establish documented procedures to safeguard that no transfer of Customer Personal Data takes place without appropriate safeguards in place.	*Please note: this Control requires a transparent documentation, such as a matrix, allowing the CSP to determine any affected transfers, where the safeguarding mechanism will be voided or requires modification, e.g., adjusted supplementary measures. Where CSP applies the identical safeguards to any transfer, the identification of such fact may be reasonable. Where CSP applies other generic rules, which allow the identification of applicable safeguards, e.g., per subprocessor, per country, this might also be considerable. In any case: the CSP shall provide information, how CSP ensures to being able to ultimately identify affected transfers in case of need.*	
	5.4.E.1. **If the destination of a data transfer is outside the EEA, does the CSP have procedures in place that note the country of destination?** Yes / No	
	a. Which procedure?	
	b. On which safeguard is this procedure based?	
	c. To the extent that more than one safeguard is relied upon for transfers of Customer Personal Data (please refer to response provided to Control 5.4.C), and there is no overarching safeguard, please provide a transparent documentation (e.g., a matrix) which allows the CSP to determine any affected transfers should the safeguarding mechanism be voided or require modification.	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	5.4.E.1.1 **Does the CSP have procedures in place to prevent transfers of Customer Personal Data to destinations outside the EEA not subject to adequacy decisions and where appropriate safeguards are not in place?** Yes / No	
	a. Which procedure?	
	b. Please explain further.	
[5.4.F] If the CSP is not established in a Member State of the European Union but in scope of the GDPR by virtue of Article 3.2, it must designate a representative in accordance with Article 27 GDPR.	5.4.F.1. **Is the CSP established in the European Union?** Yes / No	
	a. Please indicate explicitly which establishment.	
	b. Please indicate the Member State.	
	5.4.F.2. **If the CSP is not established in the European Union, please confirm whether a representative in accordance with Article 27 GDPR has been appointed.** Yes / No	
	a. If a representative has not been appointed, please provide the reasoning and exception applicable.	
[5.5.A] CSP shall provide the Customer, if	*Please note that a "**not applicable**" would be sufficient if this is not applicable to the CSP.*	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
available, an executive summary of independent third party audits and the certification of the CSPs compliance with its obligations under the Code.	5.5.A.1. **Does the CSP make executive summaries of independent third party audits available to Customers or provide it to them, upon request?** Yes / No	
	a. Please indicate the applicable mechanism put in place for such request.	
	b. Please indicate how the summaries are provided (e.g., email, publicly available on the website etc.).	
[5.5.B] CSP shall provide the Customer with any certificates, attestations or reports resulting from independent accredited third-party audits of the Cloud Services relating to security and/or personal data protection.	5.5.B.1. **Does the CSP provide the Customer with the most recent certifications or summary audit reports relating to its security measures, at least upon request?** Yes / No	
	a. Please indicate the applicable mechanism put in place for such request.	
	b. Please indicate how the certifications or reports are provided to the Customers (e.g., email, publicly available on the website etc.).	
[5.5.C] CSP's procedures regarding Customer-requested audits shall be defined, documented and transparently communicated to the Customer and, where applicable, the mandated auditor.	5.5.C.1. **Does the CSP have in place procedures regarding Customer-requested audits?** Yes / No	
	a. Please provide further details on such procedures (e.g., confidentiality and security of the premises, minimising risk of disruption to CSP's business, written notice, defined scope etc.).	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	5.5.C.1.1 **Does the CSP transparently communicate such procedures to the Customer?** Yes / No	
	a. Please explain.	
	5.5.C.1.2 **Does the CSP require a specific procedure for the Customer to request an audit (e.g., signing a specific document or form, option on the Customer Portal, etc.)?** Yes / No	
	a. Please provide details.	
[5.5.D] CSP shall provide the Customer with the means to make requests for additional evidence of compliance of the Cloud Services to this Code or to the requirements of the GDPR, where this evidence is not provided by other means.	*Please note: this Control is not necessarily limited to a Customer Audit Right. It also affects general assistance. If a CSP provides additional evidence, where necessary, only by means of a Customer Audit Right, CSP should provide information why this is not considered unduly complex for Customers, be it from a procedural or from a cost perspective.*	
	5.5.D.1. **Does the CSP provide assistance to the Customer to request additional evidence of compliance?** Yes / No	
	a. Please provide a high-level summary of the assistance provided to the Customer as related to Control 5.5.D.	
[5.5.E] If and to the extent Customer will have to bear any costs related to the performance of its audit right, such costs must not be prohibitive or excessive.	*Please note: either provide – where applicable – your static price list, or an explanation of how the costs will be determined. It might also be worth noting, if there are any specific approaches in regards of pricing, where Customers conduct such Customer Audit only in context of a supervisory authority's request or in case of reasonable doubts of conformity, such as following a notified data breach or related media reports.*	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	5.5.E.1. **Does the CSP charge its Customers for exercising its audit rights?** Yes / No	
	a. If so, please provide your static price list or an explanation of how the costs will be determined (i.e., methodology to determine the costs).	
	b. How is the cost communicated to the Customer (e.g., already included in the Cloud Service Agreement, a quote is sent when a request is received,...)?	
	c. When is the cost communicated to the Customer (e.g., at the audit request, at the contract signature, etc.)?	
[5.5.F] The CSP shall – if not covered by the Cloud Service Agreement already – have in place either additional Customer Audit Provisions or documented procedures to individually draft such Customer Audit Provisions in case of need.	*Please note: This Control requires, that Customers can easily access relevant information on the procedural and contractual provisions to conduct a Customer Audit. Such procedures and provisions usually cover elements such as prior notification, means on concluding a Customer mandated auditor (non-competition clause), etc. If not covered by the Cloud Service Agreement already, please indicate any additional documents and how Customers can access those.* *Please indicate "**not applicable**" if Customer Audit Provisions are already covered by the Cloud Services Agreement.*	
	5.5.F.1. **If not covered by the Cloud Services Agreement, does the CSP have in place additional Customer Audit Provisions or procedures to draft such provisions if needed?** Yes / No	
	a. Which provision or procedure?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	b. Please provide relevant details of such procedure.	
[5.6.A] CSP shall ensure that in case of any future disputes with its Customers CSP will comply with this section of the Code.	*Please confirm, that you will abide by the law, especially GDPR, in case of disputes with your Customers in future.* ***Please note that in case of Level 3 adherence**, this confirmation needs to be provided by the CSP and not the Third-Party Auditor.*	
	5.6.A.1 **Does the CSP confirm that it will abide by the law, especially GDPR, in case of disputes with its Customers?** Yes / No	
[5.7.A] CSP shall establish documented procedures to assist the Customer for fulfilling data subject access requests.	5.7.A.1. **Does the CSP provide the Customer with the ability to address data subjects access requests from a technical perspective (i.e., through self-service functionalities)?** Yes / No	
	a. Which documentation is provided to the Customer to support them in this regard?	
	b. Which additional support is provided to the Customer, to the extent the Customer requires additional information (beyond the documentation in a)?	
	5.7.A.2. **If no self-service functionalities are provided, does the CSP provide reasonable assistance to the Customer in addressing data subjects access requests?** Yes / No	
	a. Please provide details regarding such reasonable assistance.	
	b. Which procedure or policy establishes such assistance?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.7.B] CSP shall establish procedures or implement appropriate measures to support Customer to fully address data subject rights requests in a timely manner, including data subject access requests.	5.7.B.1. **Does the CSP provide the Customer with the ability to gather, modify or delete Customer personal data from a technical perspective (i.e., through self-service functionalities)?** Yes / No	
	a. Which documentation is provided to the Customer to support them in this regard?	
	b. Which additional support is provided to the Customer, to the extent the Customer requires additional information (beyond the documentation in a)?	
	5.7.B.2. **If no self-service functionalities are provided, does the CSP provide reasonable assistance to the Customer in gathering, modifying or deleting Customer Personal Data?** Yes / No	
	a. Please provide details regarding such reasonable assistance.	
	b. Which procedure or policy establishes such assistance?	
[5.7.C] CSP shall establish and make available to Customer communication channels by which the Customer may address its questions and requests regarding data protection measures.	5.7.C.1. **Does the CSP enable the Customer to submit requests and questions regarding the CSP's data protection measures?** Yes / No	
	a. How does the CSP make available the respective communication channel for such requests and questions?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.7.D] CSP shall establish documented procedures to assist Customer with Data Protection Impact Assessment.	5.7.D.1. **Does the CSP have procedures in place to enable assistance to the Customer regarding Data Protection Impact Assessments?** Yes / No	
	a. Please explain how such assistance is provided (e.g., details of subprocessors, provision of reports and certifications, information regarding technical and organisational measures etc.).	
[5.7.E] CSP shall establish documented procedures to ensure that no information provided to Customer in assistance of Customer's DPIA create a security risk themselves; where CSP considers information confidential CSP shall document such information and its arguments why CSP considers this information confidential. To the extent it does not create security risks and to balance interests CSP may disclose confidential information under confidentiality agreements.	5.7.E.1. **Does the CSP have procedures in place to classify information?** Yes / No	
	a. Which procedure?	
	b. How is this procedure applied when providing the Customer with information to assist them with a Data Protection Impact Assessment?	
	5.7.E.1.1. **To the extent that the CSP cannot provide information (not even subject to a confidentiality agreement), does the CSP assist the Customer by any other means?** Yes / No	
	a. Which means?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.7.F] CSP shall communicate available information with regards to data formats, processes, technical requirements and timeframes of retrieving the entrusted Customer Personal Data provided by the Customer to the CSP.	5.7.F.1. **Does the CSP have established processes in place to communicate available information with regards to data formats, processes, technical requirements and timeframes to the Customer?** Yes / No	
	a. Which processes?	
	b. How is such information communicated to the Customer?	
[5.8.A] CSP shall maintain an up-to-date and accurate record of all activities carried out on behalf of the Customer containing all required information according to Article 30.2 GDPR.	5.8.A.1. **Does the CSP maintain an up-to-date records of processing activities (ROPA) on behalf of the Customer (Art. 30.2 GDPR)?** Yes / No	
	a. Does the ROPA include, at a minimum, the name and contact details of each Customer; the categories of processing carried out on behalf of the Customer, the list of subprocessors who carry out certain activities on behalf of the CSP; transfers of Customer Personal Data to a third country and the underlying documentation of suitable legal safeguards to secure the transfer? Yes / No	
	b. Please provide a screenshot or redacted version of your ROPA as Processor.	
[5.8.B] CSP shall establish appropriate procedures that enable the Customer to provide the CSP with information necessary for the CSP's records of processing.	5.8.B.1. **Does the CSP have procedures in place to enable the Customer to provide the CSP with relevant information, in order to keep the CSPs records of processing activities be up-to-date and accurate?** Yes / No	
	a. Which procedure?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	b. Please provide a high-level summary of such procedure as it relates to Control 5.8.B.	
[5.9.A] CSP shall designate Data Protection Point of Contact with competencies according to Chapter IV, Section 4 GDPR.	5.9.A.1. **Has the CSP appointed a Data Protection Point of Contact?** Yes / No	
	a. Please confirm that a Data Protection Point of Contact is appointed in accordance with competencies according to Chapter IV, Section 4 GDPR i.e., Data Protection Officer. Yes / No	
[5.9.B] The contact data of Data Protection Point of Contact shall be communicated and available to the Customer – where required by GDPR –competent supervisory authorities, and upon request to data subjects.	5.9.B.1. **Does the CSP communicate and make the contact of the Data Protection Point of Contact available to the Customer - and where required by GDPR - competent supervisory authorities, and upon request data subjects?** Yes / No	
	a. In which documentation is this information made available (e.g., public website, policy shared with Customers,…)	
	b. What is the mechanism put by the CSP to allow the Customers to contact the Data Protection Point of Contact (e.g., email address, submission form, portal,…)?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.10.A] CSP shall establish documented procedures on how to address data subjects' requests.	5.10.A.1. **Does the CSP have procedures in place which outline how Customer data subjects' requests are handled by the CSP, taking into account the nature of the processing?** Yes / No	
	a. Which procedures?	
	b. Please provide a high-level summary of the procedure as related to Control 5.10.A.	
[5.10.B] CSP shall establish documented procedures assisting the Customer for fulfilling data subject requests, taking into account the nature of the processing.	5.10.B.1. **Does the CSP have established procedures in place to assist the Customer to fully address data subject access requests, taking into account the nature of the processing?** Yes / No	
	a. Which procedures?	
	b. Please provide details such assistance.	
[5.11.A] CSP shall establish policies and procedures to enable Customer to respond to requests by supervisory authorities.	5.11.A.1. **Does the CSP have policies and procedures in place which outline how the Customer can access the relevant information to enable the Customer to respond to requests by supervisory authorities, regarding the processing of Customer Personal Data by the CSP (e.g., making available relevant certificates or audit reports, ensuring the Data Protection Point of Contact is available, etc.)?** Yes / No	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
	a. Which procedures?	
	b. Please provide a high-level summary of the assistance provided to the Customer as it relates to Control 5.11.A.	
[5.11.B] CSP shall establish documented procedures to respond to requests by supervisory authorities ensuring that such response take place in due time and appropriate detail and quality.	5.11.B.1. **Does the CSP have policies and procedures in place to enable the CSP to gather relevant information ensuring that the CSP is able to respond to supervisory authorities in appropriate quality and due time?** Yes / No	
	a. Which policy or procedure?	
	b. Please provide a high-level description of the policy or procedure as it relates to Control 5.11.B.	
[5.11.C] CSP shall establish documented procedures to notify the Customer when it receives a request from the supervisory authority relating to Customer Personal Data, if permitted by law.	5.11.C.1. **Does the CSP have procedures in place to notify the Customer, if permitted by law, when the CSP receives a request from the Supervisory Authority relating to Customer Personal Data?** Yes / No	
	a. Which procedure?	
	b. Please provide the details of such notification.	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.12.A] CSP shall require that employees and contractors involved in the processing of the Customer Personal Data are subject to appropriate confidentiality obligations prior to engaging in such data processing activities.	*Please keep in mind: the Control addresses both employees and Contractors.*	
	5.12.A.1. **Does the CSP require its employees involved in the processing of Customer Personal Data to be subject to appropriate confidentiality obligations?** Yes / No	
	a. Which agreement ensures the confidentiality obligations of the CSP's employees?	
	5.12.A.1.1 **Does the CSP require its contractors involved in the processing of Customer Personal Data to be subject to appropriate confidentiality obligations?** Yes / No	
	a. Which agreement ensures the confidentiality obligations of the CSP's contractors?	
[5.12.B] CSP shall document organizational policies and procedures to ensure that employees and contractors involved in the processing of the Customer Personal Data are aware of their confidentiality obligations regarding Customer Personal Data.	*Please keep in mind: the Control addresses both employees and Contractors.*	
	5.12.B.1. **Does the CSP have policies and procedures in place to ensure that employees and contractors involved in the processing of the Customer Personal Data are aware of their data protection, confidentiality and security obligations?** Yes / No	
	a. What do these policies and procedures entail?	
[5.12.C] CSP shall establish policies and guidelines to ensure that Customer Personal Data is not processed by any personnel for	5.12.C.1. **Does the CSP ensure that Customer Personal Data is only processed by the CSP's personnel as requested by the instructions of the Customer?** Yes / No	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
any purpose independent of the Instructions of the Customer as provided in the Cloud Services Agreement, and/or has been explicitly requested by the Customer and/or is necessary to comply with applicable law, and/or a legally binding request.	*a. How does the CSP ensure this (e.g., documentation of Customer instructions, sign off process, workarounds, access control requirements, etc.)?*	
[5.12.D] Confidentiality obligations contained within the terms and conditions of employment or agreements with contractors or subprocessor shall continue after the end of the employment or termination of the agreement.	*Please keep in mind: the Control addresses both employees and Contractors.*	
	5.12.D.1. **Does the agreement concluded with the employees (cf. Control 5.12.A) ensure that the confidentiality obligations shall continue after the end of employment?** Yes / No	
	a. Please confirm for how long the confidentiality obligations shall continue after the end of employment.	
	5.12.D.1.1 **Does the agreement concluded with the contractors (cf. Control 5.12.A) ensure that the confidentiality obligations shall continue after the expiry or termination of the contractors' or subprocessors' agreement?** Yes / No	
	a. Please confirm for how long the confidentiality obligations shall continue after the end of the agreement.	
[5.12.E] All personnel involved in the processing of the Customer Personal Data shall receive adequate training in organizational	*Please note: This Control covers principally the data protection related dimension. Data Protection may include Cyber Security aspects. Training that are limited to Cyber Security, however, might be insufficient. Please also note: the Control requires an indication as to why the provided training is relevant for the individual role and job function of the respective personnel.*	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
policies and procedures, as relevant for their role and job function in relation to the Cloud Services.	5.12.E.1. **Does the CSP's personnel involved in the processing of the Customer Personal Data receive periodic training in organisational policies and procedures?** Yes / No	
	a. Which data protection training?	
	b. What does the training program include?	
	c. How is the training relevant to specific role and job function?	
[5.12.F] Training and awareness shall be subject to timely reviews.	*Please note: this Control addresses the material review of your training, i.e., whether the contents and the means of providing training will be reviewed, either to ensure its effectiveness or to ensure the contents' accuracy.*	
	5.12.F.1. **Are the training and awareness (cf. Control 5.12.E) subject to periodic reviews with regards to its content, its participation, its quality and effectiveness?** Yes / No	
	a. When?	
	b. How often?	
	c. What elements are subject to reviews (e.g., contents, means of providing training,...)?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.12.G] CSP shall have documented procedures to sufficiently communicate to the Customer the technical and organizational measures implemented by the CSP if to the extent the Cloud Service is capable of processing Special Categories of Personal Data.	5.12.G.1. **Are the declared Cloud Services capable of processing Special Categories of Personal Data?** Yes / No	
	5.12.G.1.1 **Has the CSP implemented technical and organisational measures (TOMs)?** Yes / No	
	a. Please provide a short explanation on the TOMs implemented.	
	5.12.G.1.2 **Have those TOMs been communicated to the Customer?** Yes / No	
	a. How?	
[5.13.A] CSP shall establish procedures to ensure the reporting of data breaches to the Customer through appropriate channels without undue delay.	*Please note: Your response should address the time-related aspect and the indication of appropriate channels.*	
	5.13.A.1. **Does the CSP have incident management procedures in place to ensure that data breaches can be reported to the Customer through appropriate channels without undue delay?** Yes / No	
	a. Please provide a high level explanation of the procedure?	
	b. Please confirm the timeline of such notification to the Customer.	
	c. Please confirm the channels through which such notifications are done(e.g., email, Customer Portal, etc.).	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.13.B] CSP shall specify its data breach notification obligations as well as its technical and organizational measures to detect, mitigate and report a data breach in the Cloud Service Agreement.	5.13.B.1. **Are the data breach notification obligations included in the Cloud Service Agreement?** Yes / No	
	a. *Please specify the CSP's technical and organisational measures to detect, mitigate and report a breach, as included in the Cloud Service Agreement*.	
[5.14.A] CSP shall provide a capability for the Customer to retrieve the Customer Personal Data promptly and without hindrance.	*Please note: Your response should address both time-related aspect and the fact that the retrieval should be done without hindrance.*	
	5.14.A.1. **Has the CSP provided a capability for the Customer to retrieve the Customer Personal Data promptly and without hindrance?** Yes / No	
	a. Can such data retrieval be done by the Customer using self-service capabilities?	
	b. To the extent no self-service capabilities are provided or cannot be used for data retrieval, how does the CSP ensure the Customer is able to retrieve Customer Personal Data promptly and without hindrance?	
	c. Which documentation ensures this (e.g., policy, procedure or cloud service agreement)?	
[5.14.B] CSP shall provide the capability for the Customer to retrieve the Customer Personal Data at the end of the provision of the	5.14.B.1 **Has the CSP provided a capability for the Customer to retrieve the Customer Personal Data at the end of the provision of the Cloud Services?** Yes / No	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
Cloud Services as covered by the Cloud Services Agreement.	*a. Can the data be retrieved by the Customer using self-service functionalities?*	
	b. To the extent no self-service capabilities are provided or cannot be used for data retrieval at the end of the provision of cloud services, how does the CSP ensure the Customer is able to retrieve Customer Personal Data promptly and without hindrance?	
	c. Which documentation ensures this (e.g., policy, procedure or cloud service agreement)?	
[5.14.C] CSP shall provide the Customer Personal Data in a machine readable, commonly used, structured format.	5.14.C.1 **Does the CSP provide the Customer with its Customer Personal Data in a machine readable, commonly used, structured format?** Yes / No	
	a. Which format?	
	b Which documentation provides the explanation on the data formats (e.g., policy, procedure or cloud service agreement)?	
	c. To the extent this can be done through self-service functionalities by the Customer, which documentation provides the explanation on how this can be done and the data formats (e.g., policy, procedure or cloud service agreement)?	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like*	Reference *e.g. to your Cloud Service Agreement, internal controls, and/or procedures, where applicable*
[5.14.D] On request the CSP shall provide the Customer a description of the format and mechanisms to provide the Customer Personal Data.	5.14.D.1. **Does the CSP provide the Customer with a description of the format and mechanisms to provide the Customer Personal Data, upon request?** Yes / No	
	a. Please explain further.	
[5.14.E] CSP shall delete all copies of the Customer Personal Data within the timescale specified in the Cloud Services Agreement, unless applicable laws or regulations require retention of that data.	5.14.E.1 **Does the Cloud Services Agreement concluded between the CSP and its Customers specify deletion and return timelines of Customer Personal Data?** Yes / No	
	a. Please indicate the timeline.	
	b. Please explain how the CSP ensures such timeline is respected.	
[5.14.F] CSP shall ensure that all storage media used to store Customer Personal Data that has been deleted have that data securely overwritten or otherwise sanitized before those media are re-used or sent for disposal.	5.14.F.1 **Does the CSP maintain an appropriate media disposal and wiping procedure to govern storage media no longer in use?** Yes / No	
	a. Which procedure?	
	b. Please provide a high level summary of the procedure as it relates to Control 5.14.F.	

Section 6

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	**Declaration** *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like.*	**Reference** *e.g. to your Cloud Service Agreement, internal controls, procedures, or third party certificates and/or audit reports, where applicable*
[6.1.A] The CSP shall apply appropriate information security measures according to the sensitivity of the Customer Personal Data contained within the Cloud Service, considering a dedicated data protection assessment perspective when assessing the appropriateness of such measures.	6.1.A.1 **Has the CSP implemented appropriate organisational and technical controls to secure data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to Customer Personal Data transmitted, stored or otherwise processed?** Yes / No *a. Please explain.*	
[6.1.B] If and to the extent the CSP is aware of the actual types or sensitivity of Customer Personal Data the CSP shall consider risks generally associated with such Customer Personal Data when assessing the appropriateness of its implemented technical and organizational measures.	6.1.B.1 **Has the CSP considered risks generally associated with Customer Personal Data when assessing the appropriateness of its implemented technical and organisation measures (to the extent the CSP is aware of the sensitivity of the Customer Personal Data)?** Yes / No *a. Please explain.*	
[6.1.C] The CSP shall establish, implement, maintain and continually improve an information security management system (ISMS), in accordance with the requirements of ISO 27001 or any equivalent International	6.1.C.1 **Please confirm whether the Cloud Services declared under this Declaration of Adherence is subject to a relevant ISO Certification (i.e., 27001, 27017, 27018 or 27701)?** Yes / No *a. Please provide the Certificate and the respective Statement of Applicability.*	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like.*	Reference *e.g. to your Cloud Service Agreement, internal controls, procedures, or third party certificates and/or audit reports, where applicable*
Standards.		
	b. Please indicate the Certificate Number.	
	c. Please confirm that all the Services declared under the EU Cloud CoC for this Declaration of Adherence are also covered by the submitted ISO Certification.	
	d. Please indicate the validity period of the Certificate.	
	e. To the extent that that validity period of the Certificate would end before the EU Cloud CoC due date of verification, please confirm that the Certificate will be renewed.	
	6.1.C.2 **To the extent the response to 6.1.C.1 is no, does the CSP confirm that the Cloud Services declared under this Declaration of Adherence are subject to another third-party report (e.g., SOC 2)?** Yes / No	
	a. Please provide the Certificate.	
	b. Please confirm that all the Services declared under the EU Cloud CoC for this Declaration of Adherence are also covered by the submitted report.	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like.*	Reference *e.g. to your Cloud Service Agreement, internal controls, procedures, or third party certificates and/or audit reports, where applicable*
[6.1.D] The CSP shall establish a process to determine the boundaries and applicability of the ISMS taking into account the nature of the respective Cloud Service. The CSP shall document its reasons why it considers any of the Controls [6.2.A] to [6.2.Q] falls outside the applicability of the Cloud Service's ISMS and thus is not implemented. Where, instead, the CSP implemented alternative measures than those required by [6.2.A] to [6.2.Q], it shall provide reasoning and evidence to the Monitoring Body why those measures adequately replace the Controls concerned.	6.1.D.1 **Could you please confirm that all EU Cloud CoC Controls (i.e., [6.2.A] to [6.2.Q]) are covered by the respective Cloud Service's ISMS.** Yes / No	
	a. Please indicate the respective ISO Certification or another applicable third-party report (e.g., SOC 2).	
	6.1.D.2 **To the extent the response to 6.1.D.1 is no, please indicate if any of the Controls [6.2.A] to [6.2.Q] falls outside the applicability of the Cloud Service's ISMS and thus is not implemented.**	
	a. Please indicate which Control are not covered.	
	b. Please indicate whether alternative measures than those required by [6.2.A] to [6.2.Q] were implemented for the Controls concerned.	
	c. Please provide reasoning and evidence to the Monitoring Body why those measures adequately replace the Controls concerned.	
Objective 1 - Management direction for information security	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like.*	Reference *e.g. to your Cloud Service Agreement, internal controls, procedures, or third party certificates and/or audit reports, where applicable*
[6.2.A] The controls set out in ISO 27001 control domain A 5 or equivalent International Standard, but no less protective, shall be implemented.		
Objective 2 - Organisation of information security [6.2.B] The controls set out in ISO 27001 control domain A 6 or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
Objective 3 Human resources security [6.2.C] The controls set out in ISO 27001 control domain A 7.1 and A 7.2 or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
Objective 4 - Asset management [6.2.D] The controls set out in ISO 27001 control domain A 8 or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
[6.2.E] The controls set out in ISO 27001 control domain A 11.2 or equivalent International Standard, but no less protective, shall	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like.*	Reference *e.g. to your Cloud Service Agreement, internal controls, procedures, or third party certificates and/or audit reports, where applicable*
be implemented.		
Objective 5 - Access controls [6.2.F] The controls set out in ISO 27001 control domain A 9 or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
Objective 6 - Encryption [6.2.G] The controls set out in ISO 27001 control domain A 10 and A13.2, or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
[6.2.H] Where the mechanism exists, CSP shall support Customer with encryption of Customer Personal Data over public networks.	*Please note: This Control is not necessarily covered by your existing certifications or attestations. Therefore, please provide a free text response.*	
	6.2.H.1 **Does the CSP have appropriate procedures to support Customers by implementing encryption in line with industry best practices and relevant regulations?** Yes / No	
	a. Which procedures?	
[6.2.I] To the extent CSP provides encryption capabilities such capabilities shall be implemented effectively, i.e. by following strong and trusted techniques, taking into account	*Please note: This Control is not necessarily covered by your existing certifications or attestations. Therefore, please provide a free text response.*	
	6.2.I.1 **Please explain the encryption capabilities provided to Customers (cf. Control 6.2.H.1).**	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like.*	Reference *e.g. to your Cloud Service Agreement, internal controls, procedures, or third party certificates and/or audit reports, where applicable*
the state-of-the-art, adequately preventing abusive access to Customer Personal Data.		
Objective 7 - Physical and environmental security [6.2.J] The controls set out in ISO 27001 control domain A 11, or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
Objective 8 - Operational security [6.2.K] The controls set out in ISO 27001 control domain A 12, or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
Objective 9 - Communications security [6.2.L] The controls set out in ISO 27001 control domain A13, or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
Objective 10 - System development and maintenance	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like.*	Reference *e.g. to your Cloud Service Agreement, internal controls, procedures, or third party certificates and/or audit reports, where applicable*
[6.2.M] The controls set out in ISO 27001 control domain A 14, or equivalent International Standard, but no less protective, shall be implemented.		
Objective 11 - Suppliers [6.2.N] The controls set out in ISO 27001 control domain A15 or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
Objective 12 - Information security incident management [6.2.O] The controls set out in ISO 27001 control domain A16, or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
[6.2.P] The CSP shall establish documented procedures to determine whether a security breach potentially resulted into a Data Breach.	*Please note: This Control is not necessarily covered by your existing certifications or attestations. Therefore, provide in any case a free text response.*	
	6.2.P.1 **Has the CSP established documented procedures to determine whether a security breach potentially resulted into a Data Breach?** Yes / No	
	a. Which procedure?	
	b. Please provide a high level explanation.	

Control *The controls do not override the Code. Read the Code carefully in each section as it may provide additional information on what is expected by the Monitoring Body.*	Declaration *Though the Control Guidance is not binding, please read such guidance carefully as it correlates with expectations of the Monitoring Body, how your implementation may look like.*	Reference *e.g. to your Cloud Service Agreement, internal controls, procedures, or third party certificates and/or audit reports, where applicable*
Objective 13 - Information security in business continuity [6.2.Q] The controls set out in ISO 27001 control domain A17 or equivalent International Standard, but no less protective, shall be implemented.	*For **Levels 2** and **3 adherence**, please indicate the applicable certification or third-party report.* *Please note that a free text response is required for **Level 1 adherence.***	
[6.3.A] The CSP shall provide transparent information in accordance with the demonstration keys of Section 6.3 of the Code.	6.3.A.1 **Has the CSP implemented mechanisms to facilitate access to generally recognised international certificates, attestations and other applicable assessments in relation to organisational and technical controls regarding the Cloud Service?** Yes / No *Related to Controls 5.5.A, 5.5.B and 5.2.B.*	
	a. Please explain the mechanisms implemented.	