EU Cloud Code of Conduct

Controls Catalogue – template for DoA

EU Data Protection Code of Conduct for Cloud Service Providers

Related Code Version:	2.11
Template Publication Date:	July 2022
Website:	https://eucoc.cloud

0 Introduction

0.1 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.

0.2 Expectations of the Monitoring Body (Examples)

As the implemented measures may materially differ between different Cloud Services and Cloud Service Providers, 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.

0.3 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.

0.4 Your To Do

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

1 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. Keep this in mind when responding, please.* *Please, also note, that in case of 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.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.		
[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.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.*	

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.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.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.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.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.		
[5.2.A] CSP shall assist Customer to comply with its obligations under Article 28 GDPR to the extent the CSP is involved in the processing of Customer Personal Data taking into account the nature of the processing and the information available 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*
[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.C] CSP shall communicate mechanisms to the Customer how to access the information of 5.2.B.		
[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.E] CSP shall establish operational mechanisms to maintain data retention policies and schedules regarding Customer Personal Data.		
[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.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].*	

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.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.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.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.*	

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.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.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.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' headquarters or places of processing.*	

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.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.	*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. Keep this in mind when responding, please.*	
[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.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.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.		

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] 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.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.	*If you consider an establishment in a Member State of the European Union to be applicable, please, indicate explicitly the establishment and the Member State.*	
[5.5.A] CSP shall provide the Customer, if available, an executive summary of independent third party audits and the certification of the CSPs compliance with its obligations under the Code.		
[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.		

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] 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.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 undue complex for Customers, be it from a procedural or from a cost perspective.*	
[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.*	
[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.*	
[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.*	

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.A] CSP shall establish documented procedures to assist the Customer for fulfilling data subject access requests.		
[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.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.D] CSP shall establish documented procedures to assist Customer with Data Protection Impact Assessment.		

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.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.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.		
[5.8.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.B] CSP shall establish appropriate procedures that enable the Customer to provide the CSP with information necessary for the CSP's records of processing.		

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*
[5.9.A] CSP shall designate Data Protection Point of Contact with competencies according to Chapter IV, Section 4 GDPR.		
[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.		
[5.10.A] CSP shall establish documented procedures on how to address data subjects' requests.		
[5.10.B] CSP shall establish documented procedures assisting the Customer for fulfilling data subject requests, taking into account the nature of the processing.		
[5.11.A] CSP shall establish policies and procedures to enable Customer to respond to requests by supervisory authorities.		
[5.11.B] CSP shall establish documented procedures to respond to requests by supervisory authorities ensuring that such responds take place in due time and appropriate detail and quality.		

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*
[5.11.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.		
[5.12.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 Controls addresses both, employees and 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 Controls addresses both, employees and Contractors.*	
[5.12.C] CSP shall establish policies and guidelines to ensure that Customer Personal Data is not processed by any personnel for 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.		

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.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 Controls addresses both, employees and Contractors.*	
[5.12.E] All personnel involved in the processing of the Customer Personal Data shall receive adequate training in organizational policies and procedures, as relevant for their role and job function in relation to the Cloud Services.	Please note: This Control covers principally the data protection related dimension. Data Protection may include Cyber Security aspects. Trainings that are limited to Cyber Security, however, might be insufficient. Please also note: the Controls requires indication why the provided trainings are relevant for the individual role and job function of the respective personnel.	
[5.12.F] Training and awareness shall be subject to timely reviews.	*Please note: this Control addresses the material review of your trainings, i.e., whether the contents and the means of providing trainings will be reviewed, either to ensure its effectiveness or to ensure the contents' accuracy.*	
[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.		
[5.13.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.	

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.		
[5.14.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.B] CSP shall provide the capability for the Customer to retrieve the Customer Personal Data at the end of the provision of the Cloud Services as covered by the Cloud Services Agreement.		
[5.14.C] CSP shall provide the Customer Personal Data in a machine readable, commonly used, structured format.		
[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.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.		

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.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.		

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 implemenation 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.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.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 Standards.		

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 implemenation 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.		
Objective 1 - Management direction for information security [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.		

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 implemenation 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 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.		
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.		
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.		
[6.2.E] The controls set out in ISO 27001 control domain A 11.2 or equivalent International Standard, but no less protective, shall be implemented.		

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 implemenation 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 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.		
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.		
[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, provide in any case a free text response.*	
[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 the state-of-the-art, adequately preventing abusive access to Customer Personal Da-ta.	*Please note: This Control is not necessarily covered by your existing certifications or attestations. Therefore, provide in any case a free text response.*	

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 implemenation 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 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.		
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.		
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.		
Objective 10 - System development and maintenance [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.		

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 implemenation 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 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.		
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.		
[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.*	
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.		

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 implemenation may look like.*	**Reference** *e.g. to your Cloud Service Agreement, internal controls, procedures, or third party certificates and/or audit reports, where applicable*
[6.3.A] The CSP shall provide transparent information in accordance with the demonstration keys of Section 6.3 of the Code.		