EU Cloud Code of Conduct

EU CLOUD COC

EU Data Protection Code of Conduct for Cloud Service Providers

Version:	2.11
Publication Date:	December 2020
Website:	https://eucoc.cloud

0 Contents

1 Introduction

Cloud computing provides significant benefits to both public and private sector customers in terms of cost, flexibility, efficiency, security and scalability. It is crucial that Customers develop a level of confidence in a Cloud Service Provider ("**CSP**"), before they entrust them with their data and applications. GDPR[1] requires that the customers only use CSPs as processors that provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.

The purpose of this voluntary EU Data Protection Code of Conduct for Cloud Service Providers, or in its short version EU Cloud Code of Conduct, ("**Code**") is to demonstrate these guarantees and make it easier and more transparent for Customers to analyse whether Cloud Services are appropriate for their use case. The Code has thus been prepared to contribute to the proper application of the GDPR, taking into account the specific features of the cloud computing sector. The heightened baseline of data protection compliance created by the Code will contribute to an environment of trust and will create a high default level of data protection in the European cloud computing market, in particular for Customers such as small and medium enterprises (SMEs) and public administrations.

The Code only applies to "business-to-business" (B2B) cloud services where the CSP is acting as a processor. It therefore does not apply to "business-to-consumer" (B2C) services or for any processing activities for which the CSP may act as a data controller.

The Code consists of a set of requirements for CSPs. The Code is supported by a Controls Catalogue available to CSPs and Supervisory Authorities and interested parties helping to assess compliance with the requirements of the Code. The Controls Catalogue maps the requirements of the Code to auditable elements ("**Controls**"), and also maps requirements of the Code to corresponding provisions of the GDPR and relevant international standards, thus facilitating its application and interpretation in practice.

Relevant Controls have been integrated throughout the text of this Code, so that any interested party can easily determine the requirements of the Code that must be implemented in practice. The Controls are thus an inherent part of the Code, and compliance with the Controls is a mandatory part of declaring adherence to the Code. Provisions that are mandatory and binding in order to reach compliance with this Code, whether defined in Code provisions or in Controls, are identified by the usage of the terms "shall" and "must". In addition, implementation guidance is provided in the Controls Catalogue as well, indicating possible ways for CSPs to implement the Controls in practice. This guidance is identified by the usage of the terms "may", "should" and "can". As such, the guidance is not binding, and CSPs may implement Controls in a different manner that achieves the same outcomes. However, the guidance provides a certain level of support for CSPs who are uncertain on how to interpret and implement Controls.

The Code is a voluntary instrument in accordance with Article 40 GDPR. In particular, this Code is an element pursuant to Article 28.5 GDPR whereby a CSP demonstrates sufficient guarantees by implementing appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR (including when engaging sub-processors). The EU Cloud Code of Conduct also addresses Article 28.2 and Article 28.3 GDPR including the references, as far as applicable for the cloud processing industry. In addition, the EU Cloud Code of Conduct addresses further articles of GDPR for the cloud processing industry, in each case to the extend as described in the Controls Catalogue. Namely, these are (all GDPR):

Art. 5.1, Art. 6, Art. 27, Art. 28.1, Art. 28.2, Art. 28.3, Art. 28.4, Art. 28.5, Art. 28.9, Art. 29, Art. 30.2, Art. 30.3, Art. 30.4, Art. 31, Art. 32,

[1] GDPR means the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Art. 33, Art. 37, Art. 39.1 (b), Art. 44, Art. 45.1, Art. 45 Art. 46, Art. 47.

Any CSP may choose to sign up any or all of its Cloud Services to the Code, irrespective of where it is established or where the Customer Personal Data is stored and processed, provided that the CSP meets all requirements of the Code with regards to the chosen Cloud Service. It is thus not mandatory for a CSP to make all of its Cloud Services subject to the Code; it can select for which Cloud Services it wishes to declare adherence. CSPs that have evaluated and demonstrated their compliance in accordance with the requirements in the Code may thereafter use the Code's Compliance Marks with regards to its adherent Cloud Services, see Section 7.6.

Prior to using a specific Cloud Service, Customers are invited to verify that the Cloud Service is declared adherent and listed in the Public Register of this Code, hence being monitored by the Monitoring Body: https://eucoc.cloud.

2 Terminology

Any terminology used in this Code, which is defined by the GDPR (e.g. personal data, controller, processor, data subject, etc.) shall have the meaning and interpretation as defined in accordance with that regulation, if not explicitly stated otherwise.

Furthermore, the following defined terms are used in the Code:

- **'Cloud Computing'**: paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand provided by a CSP.
- **'Cloud Service Provider'** or '**CSP**': party which processes personal data in its capacity as a Processor.
- **'Customer'**: party which is in a business relationship with a CSP for the purpose of using Cloud Services, either being a processor itself or the controller.
- **'Cloud Services Agreement'**: the full (set of) written agreements between the CSP and the Customer, which includes their contractual obligations, including with respect to a legally binding data processing agreement. The Cloud Services Agreement may take the form of general terms and conditions, including those published online and/or incorporated by reference into other contractual documents that apply to all Customers of the CSP's services.
- **'Cloud Services'**: one or more capabilities offered via Cloud Computing invoked using a defined interface, including but not limited to IaaS, SaaS, PaaS.
- **'Monitoring Body'**: means the accredited monitoring body, as provided in Article 41 GDPR, appointed by the Steering Board.
- **'Compliance Mark'**: the declaration of compliance attributed to a declaration of adherence in accordance with Section 7.6.
- **'Customer Personal Data'**: any personal data in relation to data subjects that the Customer entrusts to the CSP as part of the provision of the Cloud Services.
- **'Customer Portal'**: any web-accessible restricted area, where Customer may access further documents, settings and configuration, further information, dedicated information and communication channels regarding the Cloud Service concerned; e.g. via plain text, links, downloads, dashboards.
- **'Party'**: natural person or legal entity, whether or not incorporated, or a group of either.
- **'Instructions'**: documented instructions provided by the Customer to the CSP in relation to the processing of Customer Personal Data as a part of the Cloud Services. Instructions can e.g. be integrated into the Cloud Service Agreement or may be conveyed through standardised interactive interfaces or dashboards made available by the CSP to the Customer, in which the Customer can express its instructions, provided that the latter offers appropriate and auditable documentation.
- **'IaaS'**: Infrastructure as a Service
- **'PaaS'**: Platform as a Service
- **'SaaS'**: Software as a Service

3 Structure of the Code

The Code is structured as follows, with each section addressing a particular topic:

- **Scope:** describes the field of application of the Code, including the use cases for which it is particularly intended and the CSP's Cloud Services to which it may apply.
- **Data Protection:** describes the substantive rights and obligations of adhering CSPs on the basis of key principles, for instance purpose delimitations, data transfers, security, auditing, liability, data subject rights.
- **Security Requirements:** describes how the adhering CSP must ensure that its Cloud Services to which the Code applies meet a baseline of appropriate technical and organizational security measures.
- **Monitoring and Compliance:** describes the mechanisms how the requirements of this Code are monitored, CSP's compliance to the requirements of this Code is ensured and complaints may be handled.
- **Internal Governance:** describes how the Code is managed, applied and revised, including the roles and obligations of its governing bodies.

4 Scope

Any CSP may choose to declare its adherence to the Code, for any Cloud Services through which Customer Personal Data may be processed.

A Cloud Service may be provided by one CSP and supported by another, e.g. via 'subprocessor chains'. A common example is a SaaS Cloud Service from one CSP, built using an IaaS service of another CSP. In order to try to simplify compliance for the Customer, CSPs that are the sole contracting entity towards the Customer should be the main point of contact for the Customer, whilst their contracts and related documents provide Customers with needed information and disclosures related to all of the processor chains as required under this Code. Where Customers have directly contracted with multiple CSPs or other service providers, for instance to build their own applications and services, then each CSP is only responsible for the contracting and delivery of the Cloud Service they provide.

Furthermore, the nature of the Cloud Service (SaaS, PaaS, IaaS, or other) provided in public, private or hybrid clouds imply services of different nature, which may have different related data protection obligations. The Code enhances information accessible for Customers to enable them to understand the nature of the Cloud Service. Guidance is provided within the Code to help CSPs understand the nature of the Cloud Service type and the obligations related to it.

The present Code is broad enough in scope to cover all Cloud Services in which Customer Personal Data may be processed. The Code is explicitly not intended for Cloud Services in which no Customer Personal Data can be processed, and adherence for such Cloud Services cannot be declared.

5 Data Protection

5.1 Terms and Conditions of the Cloud Services Agreement

The Cloud Services Agreement between the CSP and its Customer shall determine the terms under which the Cloud Service is delivered. This Code does not replace a contract between the CSP and the Customer. However, the CSP shall ensure that the terms of its Cloud Services Agreement contain all applicable elements required under the GDPR, notably in Article 28.3. The CSP shall further ensure that the terms of its Cloud Service Agreement comply with the requirements of this Code.

For the avoidance of doubt: The Cloud Service Agreements must not undermine the provisions of this Code.

[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.

[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.

The CSP and its Customer shall remain responsible for compliance with their respective obligations under GDPR, including with regard to security measures. In case of disputes on contradictions or ambiguities between the Cloud Services Agreement and this Code, complaints may be raised and addressed in accordance with the complaint mechanisms established in the Section of the Code addressing Monitoring and Compliance (Section 7.8).

[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.

[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 its capacity as a processor, the CSP shall act only on behalf and under the Instructions of the Customer with respect to Customer Personal Data processed pursuant to the Cloud Services Agreement.

The Cloud Services Agreement shall set out the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. The Cloud Services Agreement shall also specify whether, and under what conditions, the use of subprocessors is allowed, as further discussed in Section 5.3.

[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 Processing Personal Data Lawfully

Taking into account the nature of processing and to the extent CSP is involved in the processing of Customer Personal Data, CSP shall assist Customer to comply with Customer’s obligations under Article 28 GDPR. CSP shall provide Customer with relevant information to enable Customer to comply with GDPR. In the course of the Cloud Service Agreement and to the extent CSP is concerned as processor, CSP shall not process Customer Personal Data except on Customer’s Instructions unless required to do so by law, as specified in Article 28.3 GDPR. **For the avoidance of doubt and just for transparency:** The Customer remains responsible for complying with its obligations and duties under GDPR. Notably, the Customer remains responsible for verifying whether the CSP Cloud Services comply with the Customer’s obligations under the GDPR, especially noting Customer’s own compliance requirements.

[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.

[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.

In accordance with GDPR, at the choice of the Customer, the CSP shall not retain or otherwise process the Customer Personal Data longer than necessary in order for the CSP to comply with its obligations under the Cloud Services Agreement, unless otherwise required by law. As communicated in the Cloud Service Agreement, the CSP shall either implement measures which are designed to satisfy the data retention limitation requirement regarding Customer Personal Data or, if retention is managed by the Customer, measures which enable the Customer to take steps to satisfy the data retention limitation requirement related to Customer Personal Data. Where applicable, the CSP shall make its data retention policy regarding Customer Personal Data available to the Customer.

[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.

[5.2.G] CSP shall communicate its standard retention policies and schedules regarding Customer Personal Data to its Customers.

Furthermore, at the time of termination of the Cloud Services Agreement, the CSP shall respect the requirements of this Code as set out in Section 5.14 below.

5.3 Subprocessing

The CSP may engage other processors as its subcontractors (”**subprocessors**”). Engaging a subprocessor is permissible under the requirements set out in this Section.

In accordance with Article 28.2 GDPR the CSP shall not engage a subprocessor without prior specific or general written authorization of the Customer. The authorization may be obtained in the Cloud Services Agreement.

A general authorization in the Cloud Services Agreement can authorize CSP to change subprocessors or jurisdictions without the requirement to obtain additional authorization from the Customer, subject to a prior notice to the Customer.

More specifically, the 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. In such a case the notification shall be made before that subprocessor starts to process Customer Personal Data. Notification may be made to the Customer through automated notices or other means where appropriate. Within a reasonable period of receiving such notification, the Customer may object to any such changes. If the CSP and Customer cannot find a mutually agreeable resolution to address the Customer’s objection, the Customer may terminate in accordance with the termination rights, as specified in the Cloud Services Agreement, or as mutually agreed by the Customer and the CSP. CSP shall always provide at least one effective measure for the Customer to object to any changes of subprocessors in order to prevent the respective processing (e.g. by termination of the affected Cloud Service, suspending the processing activities subject to the objected change, or by deletion of Customer Personal Data).

[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.

Where a CSP engages a subprocessor for carrying out specific processing activities related to the processing of Customer Personal Data under the Cloud Service Agreement, the CSP shall, in accordance with Article 28.4 GDPR, ensure that the same data protection obligations are in place in the relationship with the subprocessor as agreed upon between the CSP and the Customer. This means that there shall be the same contractual obligations agreed upon as those agreed by the CSP with the Customer, and the technical organizational measures provided by the subprocessor shall be no less protective than those provided by the CSP in accordance with the requirements of Article 28.3 GDPR and as set out in the Cloud Services Agreement with the Customer.

Where the subprocessor fails to fulfil its data protection obligations, the CSP shall remain fully liable to the Customer for the performance of the subprocessors' obligations.

[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.

Additionally, the CSP shall maintain an up-to-date list of subprocessors engaged by the CSP in the processing of the Customer Personal Data. The list shall include the legal name of the subprocessor entity and any jurisdictions that may apply. Additionally, the CSP may describe in that list the function of each subprocessor or any other helpful information taking into account what information may be necessary for its Customers.

Upon signature of the Cloud Services Agreement between the CSP and the Customer, disclosure of any information on the CSP's subprocessor engagements shall be made available subject to appropriate confidentiality terms. The Customer shall be made aware that the information is available and accessible. This list must also be accessible to relevant supervisory authorities upon their request.

For security reasons, i.e. to safeguard its data processing operations, the CSP may only provide Customer with general information regarding its subprocessors before entering into the Cloud Services Agreement. Such general information shall allow the Customer at least to identify applicable jurisdictions, e.g. based on the country or countries where the data will be processed by subprocessors and consequently, whenever data are sent outside of the European Union, to implement appropriate technical and organizational measures, including but not limited to inform data subjects concerned.

[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.

[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.

5.4 International Transfers of the Customers Personal Data

Disclaimer: If and to the extent not provided differently, e.g. by dedicated modules, this Code does not reflect a Code of Conduct pursuant Article 46.2 e) GDPR. Consequently and notwithstanding applicability of and the obligations under this Code, Customers and CSPs, who will be transferring Customer Personal Data to a third country outside the EEA, stay responsible for their due diligence to assess the individual appropriateness of implemented safeguards according to Chapter V of the GDPR; CSPs and Customers shall also abide by applicable judgements, such as ECJ C-311/18[2], and follow EDPB guidelines and recommendations in particular the Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[3], which might require CSPs to verify on a case-by-case basis, prior to any transfer whether the law or practice of the third country concerned allows to ensure the level of data protection required in the EEA, so as to determine if the guarantees provided by the chosen appropriate safeguards can be complied with in practice taking into consideration the possible interference created by the third country legislation with the fundamental rights.

This Code is ensuring CSPs will know their transfers and will adequately communicate such transfers to Customers, and that each transfer is safeguarded by at least one mechanism pursuant Chapter V GDPR. To the extent feasible, the CSP's obligations to cooperate with Customers as provided by Section 5.7 of this Code, shall include adequate support of Customers to perform their individual due diligence prior third country transfers. Adherence to this Code does not exempt CSPs or Customers to comply with requirements under GDPR, for example, Article 48 GDPR, which might require CSPs to integrate a process to adequately assess and – to the extent necessary – reject transfer or disclosure of Customer Personal Data.

The Customer may itself transfer[4] or provide Instructions to the CSP to transfer, on its behalf, Customer Personal Data to a third country outside the European Economic Area ("**EEA**"), as reflected in the Cloud Services Agreement.

Such international transfers shall take place only if the conditions in Chapter V GDPR are met, e.g. if either an adequacy decision pursuant to Article 45 GDPR or any other appropriate safeguard pursuant to Article 46 GDPR is in place, irrespective of whether the entity receiving the data in the third country is the CSP itself or subprocessor engaged by the CSP. Any transfers of Customer Personal Data to a third country outside the EEA undertaken by the CSP, if and so far, must be agreed upon in the Cloud Service Agreement. **For the avoidance of doubt:** Control 5.3.D applies accordingly in this regard as well.

[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.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.

[2] http://curia.europa.eu/juris/documents.jsf?num=C-311/18.

[3] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

[4] *Transfer* in this Section of the Code refers to any transfers of personal data to third countries or international organisation in the meaning of Chapter V GDPR.

[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.

[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.

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 The CSP shall grant the representative the authority to represent the CSP in particular towards supervisory authorities and data subjects, on all issues related to processing for the purposes of ensuring compliance with the GDPR.

[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.

5.5 Right to audit

5.5.1 Principle

The Customer must be able to assess whether the processing activities of the CSP are in compliance with its obligations under the Code, and under GDPR as a processor. In particular, the CSP shall make available to the Customer all information necessary to demonstrate compliance in accordance with Article 28.3 (h) GDPR, and allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.

The CSP shall implement appropriate and accessible mechanisms for providing evidence of compliance and shall make information available to the Customer in relation to these mechanisms. Where available for the Cloud Service, the CSP should provide Customers with access to independent third-party audit reports, and to the extent permissible due to the conditions of the respective third-party audit or enable self-service mechanisms for continuous monitoring.

[5.5.A] CSP shall provide the Customer, if available, an executive summary of independent third party audits and the certification of the CSP’s 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.

5.5.2 Principles for Customer Audits

In order to respect the data protection of all Customer Personal Data as well to keep implemented technical and organizational measures with regards to security whilst fulfilling its requirements under Article 28.3 (h) GDPR, the CSP may transparently communicate and specify in the Cloud Service Agreement how the CSP will fulfil its requirements under Article 28.3 (h) GDPR, without effectively limiting Customers rights thereunder. It shall take into account:

- ensuring confidentiality and security of the premises;
- minimising risk of disruption to CSP's business and other Customers;
- minimising risk of data breaches caused by the audits;
- ensuring conformity with the CSP's practices, policies and legal obligations;
- ensuring compliance with any agreements, rights or legal obligations of other Customers or their data subjects;
- requiring the Customer to provide written notice reasonably in advance of the proposed audit date;

- setting forth a defined scope for a mutually agreed audit plan.

Therefore, the CSP may e.g. choose to implement a staggered approach or self-service mechanism or a combination thereof[5] to provide evidence of compliance, in order to ensure that the Customer Audits are scalable towards all of its Customers whilst not jeopardizing Customer Personal Data processing with regards to security, reliability, trustworthiness, and availability.

5.5.3 Approach for Customer audits

The CSP may e.g. provide non-confidential information by technical means, e.g. a Customer Portal. Such information maybe a general description of the implemented technical and organisational measures as well as any third-party attestations and reports resulting from accredited independent third-party audits, such as ISO 27001, ISO 27701, SSAE SOC 2, approved codes of conduct under the GDPR, and any other industry standards as may be specified in the Cloud Services Agreement.

Where Customer requests further information, CSP may provide further details, including confidential information, provided that Customer has signed an appropriate confidentiality agreement, without prejudice to the CSP's obligation to provide to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR. Such confidential information may be unsanitized attestations or reports, for instance that result from accredited independent third-party audits.

Where Customer requests further information, the CSP may offer the Customer or its mandated auditor a security and data protection review with the CSP. If the Customer requests further information, only the Customer or its mandated auditor may conduct an onsite visit of the CSP facilities used to provide the Cloud Service, provided that the Customer and, where applicable, the mandated auditor have signed an appropriate confidentiality agreement.

5.5.4 Customers Audit Rights and Supervisory Authorities

The Customer's audit rights do not affect the competence of supervisory authorities to monitor CSP's compliance with GDPR in accordance with their legal mandate.

5.5.5 Appropriate Qualification and Expertise of Customer or Mandated Auditors by the Customer

The CSP may provide that any onsite audits may only be performed by individuals that have an appropriate level of expertise and qualification in the subject matter to perform the audit.

5.5.6 Costs related to Customer Audits

The CSP and the Customer may specify any arrangements in relation to the cost allocation for audits in the Cloud Services Agreement, provided that such arrangements are reasonable and reflect the realistic cost of the audit, consequently are not excessive or prohibitive. In the absence of any arrangements in relation to the costs and cost allocation, the costs shall be borne by the party requesting the audit; to the extent CSP is defining those costs, they still must not be excessive or prohibitive.

5.5.7 Confidentiality

If the performance of a Customer's Audit or the provisions of information to the Customer or its mandated auditor may jeopardize the overall data protection and security of the processing of Customer Personal Data, including that of other Customers, the CSP shall not make such information available to the Customer, except when such disclosure is subject to an appropriate confidentiality agreement. Non-Disclosure or Confidentiality Agreements if required, must not limit disclosure where the Customer is obliged to inform the Supervisory Authority or any other party, e.g. its own Customers. A non-disclosure agreement may provide provisions that Customer may only disclose information subject to such a confidentiality agreement if such disclosure is

- necessary and

[5] Potential elements of such staggered approach or self-service mechanism or a combination thereof are being provided in the following subsections and the Controls Catalogue, especially in the guidance of Control 5.5.D.

- the recipient is subject to a confidentiality agreement providing at least the level of confidentiality as the one being signed between the CSP and the Customer.

For the avoidance of doubt: if and to the extent Customer is required to share any information with public authorities, including but not limited supervisory authorities, Customer shall not be required to sign a non-disclosure agreement, provided that receiving authority is already bound to confidentiality by law or Customer may not require any such confidentiality agreement to be signed by the legitimately requesting authority.

Upon completion of an audit, the parties shall exchange a copy of the audit report, which shall be subject to an appropriate confidentiality agreement.

> [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.
>
> [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.
>
> [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.

5.6 Liability

Where the CSP has acted outside or contrary to lawful Instructions of the Customer, as provided in accordance with the terms of the Cloud Services Agreement, the Customer shall have the right to pursue the liability regime as set forth in the Cloud Services Agreement and in Chapter VIII GDPR, in accordance with applicable law.

The CSP acknowledges that the provisions of the Cloud Services Agreement shall not prohibit the data subject from enforcing their data subject rights in the applicable European Union Member State and pursuing effective legal remedies that are available to data subjects under GDPR.

> [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.

5.7 Cooperation with the Customer

The CSP shall reasonably assist the Customer with its obligations, as specified under Article 28 GDPR. In the event that a Customer receives a data subject rights request for Customer Personal Data processed by the CSP, the CSP shall support the Customer in responding to such requests by (1) providing the Customer with the ability for the Customer to gather, modify or delete Customer Personal Data itself, via the Cloud Services provided by the CSP or through standardised interactive interfaces or Customer Portals made available by the CSP, and/or (2) providing additional reasonable assistance in gathering, modifying or deleting Customer Personal Data, to the extent Customer Personal Data is not accessible to the Customer and/or cannot be modified or deleted by the Customer.

The CSP shall not make the Customer's right for deletion or return of the Customer Personal Data subject to the prior resolution of any issue in relation to the Cloud Services Agreement, unless there is a legal obligation for the CSP, e.g. a court decision, preventing the CSP from deleting Customer Personal Data.

> [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.

The CSP shall provide a communications mechanism, e.g. by indicating in the Cloud Services Agreement, to enable individual support to the Customer for any questions or requests it may have regarding the data protection measures covered by both the Cloud Services Agreement and this Code.

Such mechanisms can be staged, e.g. by referring first to published documentation which is available online to the Customer before making direct communications mechanisms available, and may take the form of phone numbers, e-mail addresses, online contact forms, chat systems or any other methods that allow the Customer to establish direct communications with a representative of the CSP and with the Data Protection Point of Contact as described in Section 5.9 of this Code.

[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.

Furthermore, the CSP shall cooperate in good faith with the Customer in order to assist the Customer to comply with its obligations pursuant to Articles 32 to 36 GDPR, taking into account the nature of processing and the information available to the CSP. The CSP may charge reasonable costs for assistance that go beyond its obligations as a processor under the GDPR. The CSP shall document and make available to the Customer its policies and procedures that govern its cooperation with the Customer, including any communications channels or standardised interactive interfaces or Customer Portals available to the Customer for this purpose. The CSP may provide such assistance in the form of standard documentation or audit reports available to all Customers, or in the form of standardised interactive interfaces or Customer Portals available to all Customers.

[5.7.D] CSP shall establish documented procedures to assist Customer with Data Protection Impact Assessment.

[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.

The CSP shall support the possibility for the Customer to retrieve the Customer Personal Data that it has provided to the CSP as a part of the Cloud Services. This possibility does not have to be supported where Customer Personal Data has already been destroyed or anonymised in accordance with the Cloud Services Agreement, nor is the CSP required to provide interfaces that allow the Customer to retrieve only their Customer Personal Data, separate from non-personal data which was also entrusted to the CSP. The CSP will inform the Customer in a sufficiently detailed, clear and transparent manner about the processes, technical requirements, available data formats, transfer mechanisms and transfer characteristics, required configuration at the Customer's side, and typical timeframes, and any charges that apply for customized services that go beyond GDPR requirements if the Customer wants to obtain any Customer Personal Data that it provided to the CSP.

[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 Records of Processing

The CSP shall maintain records of its processing activities that comply with the requirements of Article 30.2 GDPR. In particular the CSP shall keep records of:

- The name and contact details of each Customer (as provided by the Customer) on behalf of which the CSP is acting;
- The categories of processing carried out on behalf of the Customer;
- The list of subprocessors who carry out certain activities on the behalf of the CSP (see also Section 5.3);
- Where applicable, transfers of Customer Personal Data to a third country and the underlying documentation of suitable legal safeguards to secure the transfer;
- A general description of the technical and organisational security measures pursuant Article 32.1 GDPR.

All the records shall be available at all times to the supervisory authority upon request.

[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.

5.9 Data Protection Point of Contact

Each CSP adhering to the Code shall nominate a data protection officer[6], when required under the GDPR. When the CSP is not obliged to nominate a data protection officer the CSP shall have a point of contact for data protection related issues, meeting the requirements of Chapter IV, Section 4 GDPR, who shall perform the functions defined in the GDPR in relation to any Cloud Services declared adherent to this Code. The CSP will ensure that such a data protection officer or point of contact, regardless if an individual or a privacy team, shall remain available for the duration of its adherence to the Code and will provide related contact information in its declaration of adherence and to the Customer as "**Data Protection Point of Contact**". The Data Protection Point of Contact required under this Code does not have to meet the requirements of Article 38.3 GDPR to the extent the Data Protection Point of Contact is not also the legally required data protection officer.

[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 Rights of the data subject

The CSP and the Customer recognize that the first point of contact for data subjects to exercise their rights shall be the controller, in accordance with the GDPR.

When the CSP receives a data subject rights request, the CSP may redirect the data subject to the Customer or may notify the Customer, in each case to the extent legally permitted and feasible considering the nature of the request and the information which is lawfully available to the CSP (including any data elements that enable the CSP to link the data subject to a particular Customer).

[6] In accordance with the Article 29 Working Party's guidelines, the data protection officer functions can, in practice be performed by a team: "*Given the size and structure of the organisation, it may be necessary to set up a DPO team (a DPO and his/her staff). In such cases, the internal structure of the team and the tasks and responsibilities of each of its members should be clearly drawn up*"; Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016, as last Revised and Adopted on 5 April 2017; see http://ec.europa.eu/newsroom/document.cfm?doc_id=44100, p.14.

[5.10.A] CSP shall establish documented procedures on how to address data subjects' requests.

The CSP shall take reasonable steps that its designated Data Protection Point of Contact is easily reachable by Customers.

Taking into account the nature of the processing and the functionality of the service, the CSP shall cooperate with the Customer to help the Customer to address any data subject rights requests made by a data subject to the Customer for access, rectification or erasure, complaints, the right to data portability, the right to restriction of processing or any implementation of data subject rights without undue delay. Where such requests are manifestly unfounded or excessive, or where such support cannot reasonably be provided consistent with the functionality of the CSP's Cloud Services, the CSP may charge the Customer a reasonable fee based on administrative costs or refuse to act on the request. This can occur because the CSP is not in a position to identify the Customer Personal Data due to the nature of the Cloud Services, e.g. due to Customer managed encryption, or because Customer Personal Data has already been destroyed or anonymised in accordance with the Cloud Services Agreement.

[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 Cooperation with the Supervisory Authorities

The CSP shall cooperate in good faith, in particular to enable adequate and timely responses, with:

- the Customer and provide reasonable assistance to the Customer to enable the latter to handle a request from a competent supervisory authority regarding the processing of the Customer Personal Data as part of the Cloud Service.
- supervisory authorities in response to any requests the CSP receives directly with regards to its Cloud Services declared adherent to the Code.
- supervisory authorities in response to any requests it receives directly, related to the processing of Customer Personal Data related to a specific Customer. The CSP will notify the Customer of any such requests received from a supervisory authority that specifically relate to the processing on behalf of that specific Customer under the Cloud Services Agreement, unless such notifications are not permitted under Union or Member State law.

[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.

[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 Confidentiality of the Processing

The CSP shall ensure that any personnel involved in the processing of the Customer Personal Data (irrespective of their exact legal qualification as employees, contractors, consultants, directors, interns, interim personnel etc. of the CSP, and of any subprocessors involved in the data processing) are under the obligation to respect the confidentiality of the Customer Personal Data, as described within the terms of, for example, the employment agreement or confidentiality agreement.

[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.

[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.

Such persons shall specifically not be permitted to collect, use or otherwise process Customer Personal Data unless this is necessary for the performance of the Cloud Services, in accordance with 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. This obligation of confidentiality shall continue as long as reasonably required, taking into account the confidentiality of the data and the applicable European Union Member State Law, after their employment ends.

[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.

[5.12.D] Confidentiality obligations contained within the terms and conditions of employment or agreements with contractors or subprocessors shall continue after the end of the employment or termination of the agreement.

The CSP shall, in addition, require that personnel processing Customer Personal Data to undergo appropriate data protection training.

[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.

[5.12.F] Training and awareness shall be subject to timely reviews.

If to the extent the Cloud Service is capable of processing Special Categories of Personal Data (Article 9 GDPR), the CSP shall sufficiently communicate to the Customer the technical and organisational measures implemented by the CSP. The Customer shall have the possibility to assess the appropriateness of the technical and organisational measures implemented by the CSP to ensure a level of security appropriate to the risk of processing Special Categories of Personal Data.

[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.

In addition to a CSP's adherence, CSP shall consider compliance with applicable relevant national Member State data protection law.

5.13 Assistance with Personal Data Breaches

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed, a Customer may be obliged to notify supervisory authorities and data subjects in accordance with Articles 33.1 and 34 GDPR.

CSPs have an important role to play in their Customers' compliance with these notification obligations. The Cloud Service Agreement shall therefore include provisions whereby the CSP commits to assist the Customer in its compliance with data breach notification obligations taking into account the nature of the processing and the information available to the CSP. To support this, the technical and organisational security measures put in place by the CSP, shall contain measures that enable the CSP to detect, mitigate and report a breach of security without undue delay. These measures should address the principal steps to be followed in information security incident management, i.e. planning and preparing; detecting and reporting; assessment and decision making; providing appropriate responses; and identifying lessons learnt.

In the event the CSP becomes aware of a breach of its security, leading to a personal data breach, the CSP shall, pursuant to the timeframes specified in the Cloud Services Agreement and in any event without undue delay, notify each impacted Customer about such breach.

[5.13.A] CSP shall establish procedures to ensure the reporting of data breaches to the Customer through appropriate channels without undue delay.

[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 Termination of the Cloud Services Agreement

In accordance with Article 28.3 (g) GDPR, the CSP shall delete the Customer Personal Data stored at the end of the provision of the Cloud Services under the Cloud Service Agreement, unless the Customer explicitly chooses to receive the Customer Personal Data, stored by the CSP's Cloud Services and, upon expiry of the agreed upon designated period for Customer to retrieve its Customer Personal Data, subsequently delete the relevant Customer Personal Data.

Where specified in the Cloud Services Agreement and possible, Customer Personal Data shall be returned in a structured, commonly used and machine-readable format.

Similarly, where specified in the Cloud Services Agreement and technically feasible the CSP may, with a reasonable additional charge, assist the Customer in transferring the Customer Personal Data to another CSP.

[5.14.A] CSP shall provide a capability for the Customer to retrieve the Customer Personal Data promptly and 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.

The Cloud Service Agreement may distinguish between the termination of the Cloud Service Agreement and the termination of the provision of the Cloud Service in order to determine when the CSP shall delete or return Customers' Personal Data. After the termination of the Cloud Services Agreement, or upon expiry of the agreed upon designated period for the Customer to retrieve its Customer Personal Data after termination of the provision of the Cloud Service, the CSP shall delete any remaining copies of the Customer Personal Data within the timescale specified in the Cloud Services Agreement unless prevented from doing so by the GDPR, and/or applicable European Union Member State law, or if the data is subject to a legal hold (such as retention obligations related to record keeping for taxes, warranties).

[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.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.

6 Security Requirements

6.1 Security Requirements for CSPs under the Code

CSP shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The nature of the technical and organizational measures implemented by the CSP shall take into account the CSP's knowledge (if any) of the sensitivity of the Customer Personal Data being processed, including by considering the nature of the Cloud Service, and the impact of any Customer Personal Data breach, both on the data subjects and on the Customer, insofar as this is known to the CSP[7]. Where the CSP offers a Cloud Service, which could be used to process Customer Personal Data with a range of sensitivities, the CSP may consider offering corresponding security options, which the Customer can opt to employ when using the Cloud Service. Information on the security options available for a particular Cloud Service shall be made available prior to the conclusion of the Cloud Services Agreement.

[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.

Each CSP shall implement an information security management system (ISMS) applicable to those Cloud Services declared adherent, which meets the requirements of ISO 27001 / 27002, or of any equivalent compliance framework. **For the avoidance of doubt**: it is not mandatory for a CSP to be certified against ISO 27001 / 27002.

[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.

[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.

[7] Notably when the sensitivity of the personal data and the impact of any personal data breach are inherently linked to the type of Cloud Service being provided, or when the actual knowledge of the CSP is the result of prior negotiations between the CSP and Customer, in which the sensitivity, impact and resulting obligations of the CSP were communicated and agreed in writing.

6.2 Detailed security objectives

To ensure compliance of a Cloud Service to the security requirement of the Code, the CSP must achieve, at least, the security objectives listed below. These were drafted on the basis of recognised standards such as ISO 27001, ISO 27701, SOC 2, C5. In addition, CSPs shall demonstrate compliance with specific requirements, as further elaborated and mapped in the Controls Catalogue. Formal certification against relevant standards is recommended but not required under the Code, in order to account for the interests of small and medium-sized CSPs.

6.2.1 Objective 1 - Management direction for information security

The CSP shall have clear management-level direction and support for the security of Customer Personal Data processed by the CSP's Cloud Services.

The CSP shall have in place a management-approved set of information security policies that govern the security of Cloud Services Customer Personal Data in the CSP's Cloud Services.

> [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.

6.2.2 Objective 2 - Organisation of information security

The CSP shall have in place a management structure to manage the implementation of information security within the CSP's Cloud Services, with clear roles and responsibilities within the organisation.

> [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.

6.2.3 Objective 3 - Human resources security

The CSP shall take all appropriate steps to ensure that all employees, contractors and other individuals, within the CSP's control, who have access to Customer Personal Data, are aware of and understand their information security responsibilities and have suitable qualifications and capabilities for their roles within the CSP. CSP will have appropriate mechanisms in place to monitor and support compliance with these policies and related obligations.

> [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.

6.2.4 Objective 4 - Asset management

The CSP shall take all appropriate steps to ensure the security and confidentiality of the CSP's assets and facilities associated with the processing of Customers' data, with policies for deleting or rendering Customer Personal Data unrecoverable.

> [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 A11.2 or equivalent International Standard, but no less protective, shall be implemented.

6.2.5 Objective 5 - Access controls

The CSP shall limit access to Customer Personal Data, both in the cloud and the facilities in which the Customer Personal Data is processed, including through logical 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.

6.2.6 Objective 6 - Encryption

Where technically feasible and operationally practicable (including based on the nature of the Cloud Service), the CSP shall make available and/or implement encryption controls – at least for any transit of data – to protect the confidentiality of Customer Personal Data in the cloud, where provided for in the Cloud Services Agreement or where considered necessary based on a risk analysis.

> [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.
>
> [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 Data.

6.2.7 Objective 7 - Physical and environmental security

The CSP shall adopt physical and environmental security measures, designed to prevent unauthorized access, alteration to or destruction of Customer Personal Data in the cloud and to the related information processing facilities.

> [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.

6.2.8 Objective 8 - Operational security

To the extent the CSP is responsible for the Customer Personal Data in the operations of the Cloud Service, the CSP shall take all appropriate steps to ensure the secure operation of facilities and services that are involved in the CSP's processing of a Customer Personal Data; among the procedures to be highlighted: redundancy or internal back-ups of Customer Personal Data and controls on changes to the CSP's data processing facilities and systems that affect Customer Personal Data 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.

6.2.9 Objective 9 - Communications security

The CSP shall take all appropriate steps designed to ensure the protection of Cloud Services Customer Personal Data in the CSP's networks and in the CSP's information processing facilities and to ensure the secure transfer of such data or to implement other appropriate security measures feasible in transferring such data in the CSP's networks and processing facilities.

> [6.2.L] The controls set out in ISO 27001 control domain A13, or equivalent International Standard, but no less protective, shall be implemented.

6.2.10 Objective 10 - System development and maintenance

The CSP shall take all appropriate steps to ensure that information security is a central part of any new developments to the relevant Cloud Service assets that it uses to process Customer Personal Data.

> [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.

6.2.11 Objective 11 - Suppliers

The CSP shall take all appropriate steps to ensure that Customer Personal Data is adequately protected where the CSP's subprocessors have access to the CSP's cloud systems or assets.

[6.2.N] The controls set out in ISO 27001 control domain A15 or equivalent International Standard, but no less protective, shall be implemented.

6.2.12 Objective 12 - Information security incident management

The CSP shall develop, implement and manage policies and procedures enabling an effective response to and (where legally required) communication to the Customer, data subjects or competent authorities in relation to personal data breaches.

[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.

6.2.13 Objective 13 - Information security in business continuity

To the extent the CSP is responsible for the Customer Personal Data in the operations of the Cloud Service, the CSP shall take all appropriate steps to ensure that information security continuity, with respect to Customer Personal Data, in the Cloud Service is integrated into the CSP's business continuity management policies, procedures and systems to ensure appropriate security and availability of Customer Personal Data in adverse situations, e.g., a disaster.

[6.2.Q] The controls set out in ISO 27001 control domain A17 or equivalent International Standard, but no less protective, shall be implemented.

6.3 Transparency

The CSP should demonstrate the level of security provided by the CSP to protect Customer Personal Data processed by the CSP as part of the Cloud Services by providing relevant information about the technical and organizational measures it has in place. This obligation is notwithstanding any other obligation under this Code to assist the Customer, namely but not exhaustively Sections 5.5 and 5.7.

Demonstration keys

The CSP can meet this requirement by providing copies, upon the Customer's request, of:

- One or more documents, including any document(s) made available to Customers online or incorporated by reference into the Cloud Services Agreement, comprising the list of technical and organisational measures taking into account the risks associated with the processing of Customer Personal Data, and/or,
- Current audit reports and/or certificates of compliance to ISO or other generally recognized international standards, especially in relation to information security, and/or
- Verified compliance with the EU Cloud Code of Conduct or any other recognized codes of conduct.

[6.3.A] The CSP shall provide transparent information in accordance with the demonstration keys of Section 6.3 of the Code.

7 Monitoring and Compliance

7.1 Introduction

This section governs all provisions related to the appointment of the Monitoring Body, adherence of Cloud Services to this Code, compliance of adherent Cloud Services, and the monitoring of and complaints' handling under the Code.

7.2 The Monitoring Body

7.2.1 Appointment, Revocation and Suspension of the Monitoring Body

7.2.1.1 Appointment

Under Article 41 GDPR only entities which are accredited as a monitoring body can apply to be appointed, by the Steering Board, as Monitoring Body of this Code, as a code of conduct pursuant to Article 40 GDPR. As long as the appointed Monitoring Body has no accreditation pursuant to Article 41 GDPR, this Monitoring Body shall not verify any Cloud Service as compliant with this Code as a code of conduct pursuant to Article 40 GDPR.

7.2.1.2 Revocation and Suspension

The Steering Board shall suspend or revoke the appointment of the Monitoring Body whenever the Monitoring Body loses its accreditation. In other circumstances the Steering Board shall only suspend or revoke the appointment of the Monitoring Body in cases where the Monitoring Body is grossly negligent in its responsibilities, e.g. by gross misconduct or fraud. A revocation or suspension of the appointment of the Monitoring Body for other reasons shall only be performed under consultation with the competent supervisory authority and with a prior notification of the Monitoring Body of at least 18 months. If and to the extent the Steering Body decides to revoke or suspend the Monitoring Body, the Steering Board shall promptly and duly – i.e. prior to the final suspension or revocation – notify the Monitoring Body's competent supervisory authority.

7.2.1.3 Consequences of Revocation and Suspension

If the Steering Board suspends or revokes the appointment of the Monitoring Body, the Steering Board shall notify the Monitoring Body's competent supervisory authority prior to any such decision. The Steering Board then shall – in consultation with the competent supervisory authority – take appropriate actions.

7.2.1.4 Consequences of cease to exist in law of the Monitoring Body

If the Monitoring Body runs bankrupt or otherwise cease to exist in law, the procedure of 7.2.1.3 shall apply accordingly.

7.2.2 Functions of the Monitoring Body

The Monitoring Body, accredited in accordance with Article 41 GDPR, and appointed by the Steering Board, shall perform the following operational duties:

- Review and verify compliance of the Cloud Services declared adherent with the Code;
- Regularly monitor whether adherent Cloud Services are compliant with the Code;
- Review and decide complaints about infringements of the Code by adherent Cloud Services;
- Establish procedures and structures to deal with complaints about infringements of the Code or the manner in which the Code has been, or is being, implemented by CSPs, and transparently communicate these procedures and structures;
- Implement procedures and structures that prevent conflicts of interests;
- Take appropriate action, selecting from sanctions laid down in Section 7.9.2 or, where applicable, from the Guidelines as adopted by the Steering Board (see Section 7.9.4), against a CSP in case of an infringement of the Code or in case a CSP is not providing the information necessary to review a possible infringement of the Code to the Monitoring Body;
- Inform the competent supervisory authority of actions taken against CSPs and the reasons for taking them (see Section 7.9.5).

7.2.3 Minimum safeguards with regards to policies, procedures and structures

Without prejudice to the accreditation pursuant to Article 41 GDPR the Monitoring Body shall develop and implement appropriate policies, procedures and structures to:

- Ensure independence, for instance a minimum period of appointment, and expertise in relation to the Code for instance related to the expertise of its personnel and of the members of the Complaint's Panel;

- Allow verification of compliance for Cloud Services and to regularly monitor whether adherent Cloud Services are compliant with the Code;
- Handle complaints about any potential non-compliance of an adherent Cloud Service with the Code;
- Appointing an independent Complaints Panel; the Monitoring Body will establish it internal guidelines, which will include notably appropriate safeguards with regards to the procedure of appointment of the Complaints Panel and with the appointment of experts from multiple Member States;
- Ensure internal separation of duties within its structures, including the Monitoring Body's unit to verify and monitor Cloud Services compliance to the Code and the Complaints Panel;
- Prevent conflicts of interest, implementing, for example, safeguards that complaints and declarations of adherence or any periodical reviews are decided by different individuals;
- Ensure that, according to the requirements of the respective Compliance Mark, periodic reviews cover all requirements of the Code within a reasonable period of time;
- Ensure that expertise of individuals working for the Monitoring Body, including members of the Complaints Panel, is proven by relevant academic degrees, several years of relevant working experience and/or relevant publications.
- The Monitoring Body shall make the referred policies, procedures and structures public and available by always disclosing them in their website.

7.2.4 Confidentiality of the Monitoring Body

The Monitoring Body is allowed to use the information obtained during a review process only for purposes related to its responsibilities pursuant to the Code. The Monitoring Body including any persons working on their behalf, is bound by an obligation of confidentiality, and ensures that all information received in the context of its activities shall be kept undisclosed and adequately protected from unauthorized access and shall be deleted when no longer necessary for the purpose it was obtained, unless otherwise determined by applicable mandatory law.

7.2.5 Transparency and Documentation obligations of the Monitoring Body

Any decision or action taken by the Monitoring Body shall be documented. Such documentation shall include, at least, the decision or action, date, substantial and essential circumstances in which such decision or action were based, main reasoning and individuals responsible. This documentation shall be kept for the time a CSP is member of the Code plus any suitable period of time to safeguard the performance of powers of supervisory authorities related to Articles 40 and 41 GDPR, provided that there is no conflict with the applicable legislation of the Member State of the Monitoring Body or its competent supervisory authority (whatever is the longer period). Any further details may be governed by specific procedures of the Monitoring Body in consultation with and subject to the accreditation of the competent supervisory authority.

Upon request of the Monitoring Body in accordance with its duties and competencies under the Code, CSPs will cooperate with the Monitoring Body providing relevant information to the Monitoring Body. Breach of such obligation could amount to an infringement of the Code.

7.3 Conditions of Adherence

CSPs that consider one or more of their Cloud Services to meet the requirements set out in the Code, can submit a declaration of adherence of one or more of their Cloud Services, to the Monitoring Body and follow the procedure set out in this Code.

By submitting a declaration of adherence of Cloud Services to this Code, the CSP commits to comply with the requirements of the Code for any Cloud Services covered by its declaration. Any Cloud Services declared adherent to the Code must comply with all requirements of the Code and not only parts of the Code.

Verified adherence of Cloud Services to the Code does not absolve any CSP from having to comply with the GDPR, and/or applicable EU Member State data protection law, nor does it protect CSPs from possible interventions or actions by supervisory authorities in the course of their supervision and enforcement activities with regards to the adherent Cloud Service. GDPR and applicable Member State Law will always prevail over the Code.

Cloud Services declared adherent will undergo rigorous scrutiny by the Monitoring Body, in accordance with the requirements of the respective Compliance Mark under which the Cloud Service is declared, see Section 7.6.2.

Without prejudice to sanctions from competent authorities as foreseen in case of breaches of the GDPR and/or other legal acts, CSPs, which fail to meet the requirements of the Code, will be subject to the enforcement mechanisms as set out in this Section of the Code.

7.4 Procedure to declare a Cloud Service adherent

CPSs submit their declaration of adherence to the Monitoring Body following the procedure provided by this Code. Only a CSP that is a Member of the Code General Assembly (as described below), is entitled to submit a declaration of adherence. The procedures published by the Monitoring Body may determine that a submission declaration of adherence shall be received only by utilizing distinct templates or online forms. Any declaration of adherence, however, shall at least entail the following information:

- name of the Cloud Service declared adherent
- name of the CSP(s) that provides such Cloud Service
- contact details of the CSP(s) and the Data Protection Point of Contact
- a legally binding statement the Cloud Service declared adherent is fully compliant with all requirements of the Code.

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

The Monitoring Body shall review the declaration of adherence in due time but may not exceed 30 (thirty) working days counting from the date the Monitoring Body receives all relevant information. Once verified, the Secretariat incorporates the verified Cloud Service into the public register. The public register shall at least provide the following information:

- Cloud Service adherent to the Code;
- Date of verification of compliance;
- Level of compliance (Compliance Mark);
- Report of the assessment of compliance and given verification by the Monitoring Body;
- Due date of the verification of compliance.

The CSP is then entitled to use the report and the Compliance Mark as described in Section 7.6 below.

A CSP whose declared Cloud Service was not verified compliant by the Monitoring Body may submit a revised declaration of adherence and information, subject to the fees as approved by the General Assembly or file a complaint pursuant to Section 7.8.1.

7.5 Assessing compliance with the Code

7.5.1 Controls

In order to ensure that the Monitoring Body and supervisory authorities can verify that requirements of this Code are met by the Cloud Services declared adherent, requirements of this Code have been translated into controls. Each control is given a unique identifier (“**Control-ID**”) of the pattern Section.Subsection.Letter, e.g. 5.1.A.

For the avoidance of doubt: Wherever this Code and the Controls Catalogue (Annex A) makes use of the terms “shall” and “must”, a CSP is obliged to implement the respective provision in order to be compliant with this Code; even if the respective provision is not translated directly into a Control. Wherever this Code makes use of the terms “should”, “may” or “can”, the Code introduces examples and recommendations. It is worth noting that even in cases of non-binding provisions indicated by such terms, the examples and recommendations establish good practices and if the CSP choses an alternative implementation, in order to be compliant with this Code, the respective implementation must be as effective and no less protective than the given guidance.

7.5.2 Control Guidance

Controls shall be in place for each Cloud Service declared adherent. For each Control, where appropriate, there is also a guidance ("**Control Guidance**"). This Control Guidance is a selection of best practices on how the Control can be implemented by CSPs declaring a Cloud Service adherent to this Code.

The Control Guidance and the original requirements of the Code shall be considered by the Monitoring Body when verifying the compliance of a Cloud Service declared adherent to the Code. The Control Guidance is not mandatory, however, the same rules as described above apply and if a CSP implements alternative measures in order to be compliant with this Code, these measures cannot be less protective than those being provided by the Control Guidance.

Additionally, Controls of Section 5 have been referenced to internationally recognized standards where relevant, including ISO 27001, ISO 27018, ISO 27701, SOC 2, and Cloud Computing Compliance Controls Catalog ("C5"), in order to provide CSPs with best practices of similar areas which might act as reference and starting point when implementing specific data protection related measures.

7.5.3 Indefinite Requirements

If and to the extent the Code or a Control leaves room for interpretation, e.g. where it requires reasonable assistance, the Monitoring Body shall provide the final conclusive decision, whether the Code's requirement is being complied with. The Monitoring Body shall consider any notion provided by the Code language and as noted in 7.5.2 by existing Control Guidance.

7.5.4 Mapping to recognized standards

Controls of Section 6 have been mapped against controls of internationally recognized standards, including ISO 27001, ISO 27018, ISO 27701, SOC 2, Cloud Computing Compliance Controls Catalog ("C5"), as well as NIST SP 800-53 and NIST Cybersecurity Framework, that are considered to be equal but not less protective than the Controls of the Code.

This mapping may act as guidance for the Monitoring Body with regards to recognizing internationally standards as sufficient evidence of compliance with related Controls of the Code.

7.5.5 Controls Catalogue

The Control Guidance, mapping of each Control to internationally recognized standards, and mapping of the corresponding article of the GDPR is compiled into a separated document ("**Controls Catalogue**") (Annex A) but is an integral part of the Code.

The Controls Catalogue translates the requirements of the Code into provisions that can be monitored and verified by any party concerned, i.e. predominantly the Monitoring Body or supervisory authorities. Compliance with the referenced internationally recognised standards alone does not imply, as such, to be compliant with the Code.

As per 7.5.1, "shall" and "must" mark binding requirements. In case binding requirements of the Controls Catalogue and any part of the Code may be conflicting in order to reach compliance, the Code prevails.

7.5.6 Assessment by the Monitoring Body

Notwithstanding the powers of and requirements set-out by the supervisory authority pursuant Article 41 GDPR, the Monitoring Body shall assess whether a Cloud Service, that have been declared adherent to the Code, is compliant with the requirements of the Code - especially as laid down in the Controls Catalogue.

To the extent feasible and by no means limiting the Monitoring Body's powers as provided under GDPR, the Monitoring Body assessment process shall be based on an evidence-based conformity assessment, based on interviews and document reviews; pro-actively performed by the Monitoring Body.

To the extent the Monitoring Body is not satisfied with the evidence provided by a CSP with regards to the Cloud Service to be declared adherent to the Code, the Monitoring Body may request additional information. The Monitoring Body shall especially request additional information, if it considers the provided reasons of a CSP inadequate regarding applicability of security objectives within the CSP's ISMS, as the CSP carries the burden of proof for any derogation.

Where the information provided by the CSP appears to be inconsistent or false, the Monitoring Body shall - as necessary - request substantiation by independent reports; costs related to such substantiation shall be covered by the CSP.

With regards to internationally recognized standards, the Monitoring Body shall consider the mapping as provided by the Controls Catalogue. However, the Monitoring Body shall verify whether (a) any third-party certification or audit provided by the CSP applies to the Cloud Service concerned, (b) such third party certification or audit provided by the CSP is valid, (c) such third-party certification or audit has assessed and sufficiently reported compliance with the mapped controls of the third-party certification or audit concerned. Provided that the aforementioned criteria are met, the Monitoring Body may consider such third-party certifications or audits as sufficient evidence for the compliance with the Code.

For the avoidance of doubt: The Monitoring Body shall not verify a Cloud Service's compliance with the Code, as long as the Monitoring Body is not convincingly satisfied by the provided evidence demonstrating the Cloud Service's compliance as subject to the applicable assessment procedure.

7.6 Different Levels of Compliance and Compliance Marks

7.6.1 Entitlement to use Compliance Marks

CSP is entitled to use the applicable Compliance Mark provided that the respective Cloud Service has been both verified compliant by the Monitoring Body and listed in the Public Register. **For the avoidance of doubt**: A compliance mark must not be used prior to verification of the Monitoring Body, also, in cases, where a Cloud Service is delisted from the Public Register for whatever reason a Compliance Mark must not be used either related to this Cloud Service.

If after being verified compliant by the Monitoring Body, a dispute concerning non-compliance of such Cloud Services arises, the CSP is entitled to continue using the Compliance Mark until the Complaints Procedures pursuant to Section 7.8.2. comes to a resolution. After receiving a final outcome of non-compliance with the Code of the adherent Cloud Services concerned, the CSP must immediately cease to use the Compliance Mark with regards to those Cloud Services if imposed accordingly by the Complaints Panel pursuant to Section 7.9.2.

The EU Cloud CoC logo must not be used in any way that creates the impression of compliance with the Code. Misuse would amount into an infringement of the Code.

7.6.2 Different levels of Compliance

The Code considers different levels of Compliance in order to provide transparency to the Customers on the Cloud Services' adherence choices. The different levels of compliance relate only to the levels of evidence that are submitted to the Monitoring Body. There is however no difference in terms of which parts of the Code are covered since adherent Cloud Services have to comply with all provisions of the Code and their respective Controls.

The Code provides three different levels of compliance:

7.6.2.1 First Level of Compliance

The CSP has performed an internal review and documented its implemented measures proving compliance with the requirements of the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the requirements set out in this Code and further specified in the Controls Catalogue. The Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

7.6.2.2 Second Level of Compliance

Additional to the "First Level of Compliance", Compliance with the Code is partially supported by independent third-party certificates and audits, which the CSP has undergone with specific relevance to the Cloud Service declared adherent and which were based upon internationally recognised standards procedures. Any such third-party certificates and audits that covered controls similar to this Code, but not less protective, are considered in the verification process of the Monitoring Body. Each third-party certificates and audits that were considered in the verification process by the Monitoring Body shall be referred in the Monitoring Body's report of verification, provided that the findings of such certificates were sufficiently and convincingly reported and documented towards the Monitoring Body and only to the extent such certificates and audits are in line with the Code. The CSP must notify the Monitoring Body if there are any changes to the provided certificates or audits.

The Controls Catalogue may give guidance on third-party certificates and audits that are equivalent to certain Controls in terms providing evidence of complying with the Code.

However, to those Controls that the CSP has not provided any equivalent third-party certificate or audit, the Monitoring Body verifies that the Cloud Service complies with the Code by information originating from the CSP.

The Monitoring Body may refuse application of Second Level of Compliance if third party certificates and audit reports, that are recognized by the Monitoring Body in the verification process concerned, are not covering an adequate share of Controls of this Code; such adequate share shall be subject to the discretion of the Monitoring Body, considering e.g. the share related to the overall amount of Controls of the Code or whether a full Section or topic is being covered.

7.6.2.3 Third Level of Compliance

Identical to the "Second Level of Compliance" but Compliance is fully supported by independent third-party certificates and audits, which the CSP has undergone with regard to the Cloud Service declared adherent and which were based upon internationally recognized standards.

To the extent a CSP refers to individual reports, such as ISAE-3000 reports, the CSP shall ensure that such reports provide sufficient and assessable information and details on the actual measures implemented by the CSP regarding the Cloud Service concerned. The Monitoring Body shall, if considered necessary, in consultation with the Steering Board, define further requirements on such individual reports, such as accreditation and training for auditors against the provisions and requirements of this Code.

7.6.3 Final decision on the applicable Level of Compliance

The CSP shall indicate the Level of Compliance it is seeking for when declaring its Cloud Service adherent. **For the avoidance of doubt**: Any final decision, whether a CSP Is meeting the requirements of a specific Level of Compliance is up to the sole discretion of the Monitoring Body,

7.6.4 Conditions to use Compliance Marks

The CSP may only use the Compliance Marks with regards to the Cloud Services verified adherent to the Code. Regarding Cloud Services that are verified compliant the CSP shall integrate the Compliance Mark in its Customer facing communication, e.g. its communication related to compliance with international standards. The Compliance Marks shall only be used in combination with the unique Verification-ID assigned by the Monitoring Body. Where technically possible, the Compliance Mark shall link to the public register of the Code; otherwise the CSP shall provide at least a footnote explaining the safeguards entailed by the respective Compliance Mark and a reference to the public register. Where the Compliance Mark as such cannot be integrated, either due to technical circumstance or in accordance with the overall design of a CSP presentation, the CSP shall at least integrate a text-reference to its adherence to the Code, providing equally transparent information. In consultation with the Steering Board the Monitoring Body shall provide further details and templates to prevent any confusion of the market, both for the use of the Compliance Mark and potentially necessary text-alternatives. Misuse, as well as breach of the aforementioned conditions could amount into an infringement of the Code.

7.7 Monitoring and enforcement

7.7.1 Monitoring

The compliance of any Cloud Service that has been declared its adherence to the Code will be monitored by the Monitoring Body as noted above.

Compliance of adherent Cloud Services shall be reviewed every twelve months unless

a) any significant changes occur to adherent Cloud Services,

b) In reaction to a Customer complaint, an adverse media report or anonymous feedback about a CSP which has declared a Cloud Service adherent to the Code;

in which case the Cloud Service shall be reviewed earlier.

Each individual annual revision does not need to cover all requirements of the Code; however, over successive reviews, all requirements of the Code will be covered. Notwithstanding the aforementioned, the adherent Cloud Service must comply with all requirements of the Code at all times and the Monitoring Body may – at all times – perform a full assessment.

If and to the extent annual revisions are not covering all requirements of the Code, the selection of such requirements shall follow definite criteria defined by the Monitoring Body and accredited by the competent supervisory authorities; such criteria may relate to the risk of processing, the technical specificities of the Cloud Services concerned, and the assurance, that all randomly assessed requirements will in due time cover all requirements of the Code.

Not submitting the compulsory annual, renewal of a declaration of adherence shall be considered as infringement of the Code if to the extent the CSP has not terminated its adherence consistent with the provisions of this Code and the procedures established by the Monitoring Body.

7.7.2 Enforcement

If the Monitoring Body becomes aware of any non-compliance of an adherent Cloud Service, the Monitoring Body can request the CSP to take specific measures ceasing any further infringement by the Cloud Service concerned. Therefore, the Monitoring Body shall notify the Complaints Panel, which then shall take the appropriate action with regards to the sanctions and remedies pursuant to Section 7.9; this procedure only applies if the Cloud Service is listed as current and verified as compliant.

In the event that the verification of compliance of a Cloud Service is revoked, the Secretariat shall delete that particular Cloud Service from the public register; the Monitoring Body shall inform the competent supervisory authority accordingly. The CSP shall cease to make reference to the Code or the Compliance Mark with regards to the Cloud Service concerned in any of its documentation or publications, including its website.

7.8 Complaints Handling and Procedures

7.8.1 Complaints of CSPs Members against decisions of the Monitoring Body

CSPs may file a complaint against any decision taken by the Monitoring Body.

Complaints against any rejection of the verification of compliance with the Code shall be addressed to the independent Complaints Panel of the Monitoring Body. The independent Complaints Panel, see Section 7.9.1, re-assesses the compliance of the declared Cloud Service based on the information presented to the Monitoring Body and either verifies the Cloud Services compliance or confirms the prior rejection.

7.8.2 Complaints against any CSP and its Cloud Services' compliance

If a Customer has reservations regarding a CSP's compliance with the requirements of this Code, the Customer is encouraged to contact the CSP first in order to obtain a mutually satisfactory solution.

If no such solution can be found, and else, the Customer can submit a complaint to the Monitoring Body. Such a complaint may be filed by any other party, such as data subjects, regardless whether such party is a Customer of the respective Cloud Service, or even anonymously.

The Monitoring Body shall review the complaint, require the CSP to provide any relevant information for the purposes of fact finding, and initiate a complaint handling process, in which its independent Complaints Panel, see Section 7.9.1, will determine whether the complaint was justified. In case the Complaints Panel concludes that the complaint was justified the Monitoring Body will in accordance with the Complaints Panel take appropriate actions to stop any further non-compliance of the adherent CSP.

The Complaints Panel will process complaints, establish whether violations of the Code have occurred and decide on possible sanctions and remedies in accordance with the sanctions and remedies provided under this Code. The Complaints Panel is part of the Monitoring Body and its members will be appointed by the Monitoring Body.

To the extent the Monitoring Body considers further detailed procedures governing complaints handling necessary, and such procedures have been accredited by the competent supervisory authority, such procedures shall be publicly available.

7.8.3 Costs and Fees related to Complaints

7.8.3.1 Costs for Complainants

As a rule, complaints can be submitted free of costs for the complainant. However, the Monitoring Body may define costs for complainants, where appropriate, to avoid potential abuse due to manifestly unfounded or excessive complaints, in particular if they are recurring. For example, in such cases the Monitoring Body may charge a reasonable fee related to its administrative costs, or simply refuse to act on the complaint. The Monitoring Body shall be able to reason its actions related to the manifestly unfounded or excessive character of the request and – subject to the accreditation of the competent authority - appropriately notify the competent authority of such cases.

7.8.3.2 Costs for CSPs - Rule

The costs for the performance of the Complaints Panel shall be covered by the service fees paid by CSPs to the Monitoring Body and the adequate share of the annual Membership Fees pursuant Section 8.3.3.

Costs related to complaints shall be borne by the CSP whose Cloud Service is concerned; such additional costs may include on-site reviews, requested, and Monitoring Body appointed third party reports, to substantiate the compliance with the requirements of the Code, travel expenses, and similar.

7.8.3.3 Costs for CSPs in case of justified complaints

If a complaint is justified in accordance to 7.8.1 and 7.8.2 by the Complaints Panel, the applicable CSP shall pay the costs that result from handling of such Complaint, including those costs that would be covered by the service and membership fees in Section 8.3.3. In those cases, the Complaint may be subject to fees, which shall be cost-based pricing and approved by the General Assembly.

The General Assembly may - in consultation with the Monitoring Body - decide upon a fixed Complaints Fee; if the General Assembly decides upon such fees, they shall be reviewed annually to ensure that the Complaints Fee mainly covers the overall costs of the Monitoring Body and its Complaints Panel. The applicable CSP shall cover the complaints costs without prejudice to other potential sanctions imposed by the Monitoring Body and its Complaints Panel, pursuant to Section 7.9.

7.9 Sanctions, remedies and notification of the supervisory authority

Without prejudice to the tasks and powers of the competent supervisory authority and the provisions of Chapter VIII GDPR, the Monitoring Body shall take appropriate actions with regards to sanctions and remedies against any CSP whose Cloud Service declared adherent is non-compliant with the requirements of this Code or who refuses or fails to cooperate with the Monitoring Body in performance of the Monitoring Body's tasks under this Code and GDPR appropriately.

7.9.1 Independent Complaints Panel

To prevent any conflicts of interests the Monitoring Body shall establish an independent Complaints Panel, an independent body within the Monitoring Body, to prevent the Monitoring Body to potentially decide upon its own, prior assessments and decisions.

The Complaints Panel shall document the facts found by the Monitoring Body, the reason to consider that facts result in non-compliance of the Code, every action taken and an explanation for such action taken.

7.9.2 Sanctions and Remedies

If a Cloud Service declared adherent to this Code is non-compliant with any requirement of the Code, the applicable CSP shall be subject to appropriate sanctions and remedies. By imposing sanctions and remedies the Monitoring Body, through the Complaints Panel, shall consider the following aspects when assessing the appropriateness of each action:

- severity of non-compliance with regards to the potential impact on level of data protection related to the personal data processed, including the potential impact on the freedoms and rights of data subjects;
- culpability of the CSP - whether the CSP intentionally disrespected the requirements of the Code or negligently misinterpreted them;
- frequency of non-compliance - has it been the first breach or have there been similar incidents before.

Based on the aforementioned criteria the Monitoring Body, through its Complaints Panel, shall impose sanctions and remedies that can be one or any combination of the following:

- non-public but formal reprimand;
- public announcement of the non-compliance, including facts and reasoning;
- temporary or permanent revocation of the verification of compliance with the Code related to the Cloud Service concerned;
- temporary or permanent revocation of the verification of compliance with the Code related to all Cloud Services the CSP;
- temporary or permanent revocation of membership in the General Assembly.

7.9.3 Procedural Principles

Notwithstanding any procedures as defined by the Monitoring Body and subject to the accreditation pursuant Article 41 GDRP, the following shall apply, at least: If and to the extent the Monitoring Body determines a non-compliance of a CSP, either within the course of assessments or due to the processing of a complaint, and consequently the Complaints Panel decided upon an appropriate sanctions and / or remedy, the Monitoring Body shall document its decisions and reasons for taking them, including non-public but formal reprimands. The Monitoring Body shall communicate its decisions and actions taken to the CSP concerned by documented and traceable means, including electronic communication such as email. If and to the extent remedies are being requested, the Monitoring Body shall – to the extent feasible – re-assess compliance with such requests in due time, considering the nature of non-compliance concerned. Decisions of the Complaints Panel shall have, if and to the extent not provided differently in the individual decisions or by this Code, immediate effect; this includes the publication of any non-compliance if and to the extent the Complaints Panel decided this to be appropriate, notwithstanding any requirements of aggregated publication of any actions taken pursuant to the accreditation of the Monitoring Body pursuant Article 41 GDPR.

7.9.4 Guidelines for Sanctions and Remedies

To safeguard comparability and coherency of sanctions and remedies imposed to CSPs, the Steering Board may adopt guidelines proposed by the Monitoring Body governing sanctions and remedies or ranges thereof to be imposed on CSPs. Those guidelines shall be drafted, approved and frequently reviewed by the Monitoring Body taking into account the practical experiences of the Monitoring Body with regards to non-compliance of CSPs and their Cloud Services declared adherent with this Code as well as expectations of the Members. The guidelines shall at least enlist and name the individual aspect of non-compliance as well as the sanctions and / or remedies to be expected. The determination of sanctions and remedies shall be chosen from the potential sanctions mentioned in this Code as well as those aspects to be taken into account by the Monitoring Body to assess the appropriateness of any sanction and remedy, for both see Section 7.9.2.

To the extent not already covered by the procedures as defined by the Monitoring Body to receive its accreditation pursuant Art. 41 GDPR, such guidelines shall also cover appropriate periods of response and implementation of imposed remedies, including consequences of non-compliance with such periods by CSP and appropriate actions and timeframes for escalation of sanctions.

In order to prevent any conflicts with the independence of the Monitoring Body, the Monitoring Body shall take such guidelines into account by imposing any action against a CSP. In case the Monitoring Body considers the provided guidance as inappropriate the Monitoring Body may at all times deviate, provided that the Monitoring Body explicitly states its deviation in its decision together with appropriate reasoning why such deviation seemed inevitably. Such a decision shall result into a review of the guidelines.

7.9.5 Notification of and cooperation with the supervisory authorities by the Monitoring Body

Without prejudice to Article 41.4 GDPR, the Monitoring Body shall proactively and in due time notify the competent supervisory authority of sanctions and remedies imposed on CSPs and the reasons for taking them, including non-public but formal reprimands.

In cases any supervisory authority concerned reaches out to the Monitoring Body that actions taken by the Monitoring Body remain behind what supervisory authorities expect as appropriate action, the Monitoring Body will take this feedback into account for any future decision to be taken. Especially to the extent supervisory authorities frequently reach out to the Monitoring Body related to the same field of action, the Monitoring Body shall – to the extent possible – adjust its procedures and internal guidelines accordingly; to the extent the Monitoring Body may not adjust its procedures or internal guidelines accordingly, e.g. as such adjustments require modifications to the Code, the Monitoring Body shall reach out to the competent body within the Code – at least the Steering Board, Section 8.1.2.

8 Internal Governance

This Section of the Code intends to enable a sustainable model of governance at multiple levels:

- Firstly, the governance of the organisational framework of the Code itself and its bodies, through a General Assembly, a Steering Board with operational decision-making power and a Secretariat for administrative support. This includes rules for the composition, recognition, tasks and oversight of all of these bodies.
- Secondly, the governance of the Code itself, ensuring that it can be updated to reflect the GDPR and ensuring that lessons learned in the

interpretation and application of the Code can be appropriately integrated.

This governance system is envisaged to be put in place progressively and in a transparent way, building on the input of relevant stakeholders. Organisations interested in being part of the governance will be invited to express their interest to the General Assembly.

8.1 Organizational framework of the Code and its bodies

The Code Governance Bodies are tasked with the implementation and administration of the Code.

8.1.1 Code General Assembly

8.1.1.1 Composition and representatives

The General Assembly is composed of the founding members – Alibaba Cloud, Fabasoft, IBM, Oracle, Salesforce and SAP – and all other members, whose applications to join have been approved by the General Assembly, provided that each of the members (the "**Members**"):

- Provide at least one Cloud Service, which might be eligible for adherence to the Code;
- Explore the possibility of declaring the adherence to the Code of at least one Cloud Service within an appropriate timeframe;
- Publicly declare their support to the principles of the Code;
- Provide operational support to the Code as agreed by the General Assembly;
- Provide financial support to the Code, as agreed by the General Assembly, in particular by continuing paying the membership fees for minimum of 24 (twenty-four) months period and declaration of adherence fees and any other fees that might be decided upon in future.

For the avoidance of doubt, being a Member of the General Meeting does not qualify a CSP as being compliant with the Code. For that purpose, CSPs must submit their declarations of adherence, for one or more of their Cloud Services, to the Monitoring Body and follow the procedure provided by the Code.

Each CSP, Member of the General Assembly is entitled to one vote, even though Members may be represented by more than one individual named persons, which should have a proven expertise in the area of cloud computing and/or data protection and should also have a strong understanding of the cloud computing business models. Each Member shall inform the Chairman of the General Assembly, prior to each General Assembly, of who their representatives are.

A CSP may cease to be a Member of the General Assembly, by giving the Chairman of the General Assembly 18 (eighteen) months prior notice and promptly paying membership fees during that period. If a Member fails to comply with the 18 (eighteen) months prior notice period (for whatever reason including exclusion), that Member shall pay the membership fees applicable to the remainder of the 18 (eighteen) months' notice period.

8.1.1.2 Powers

The General Assembly shall have the powers to designate the Chairman of the General Assembly and the members of the Steering Board; to approve annual membership fees, Supporter fees and any other fees as proposed by the Steering Board; to approve new Members; to decide on temporary or permanent revocation of membership within the General Assembly any Member following unremedied breach of the Code which is not a breach of Section 5 and 6; to approve changes to the Code, and to decide on any other matters as requested by the Steering Board.

8.1.1.3 Chairman of the General Assembly

The Chairman of the General Assembly shall be elected by the General Assembly meeting for a term of two years, with the possibility of renewing its mandate for any number of successive additional two-year terms.

8.1.1.4 Convene the General Assembly

- The General Assembly may be convened, on first call, by email sent with at least five days' prior notice and, on second call, by email sent with at least two days' prior notice.

- A Member of the General Assembly shall be deemed to have been regularly convened if the notice is sent to the email address, which the Member had beforehand informed in writing the Chairman of the General Assembly, copying the Secretariat.
- The Chairman shall convene one annual General Assembly, during the first quarter of each civil year, to approve at least annual fees, and to appoint the Chairman of the General Assembly and the members of the Steering Board, whenever applicable. The Chairman shall also convene a General Assembly, upon request of any member of the General Assembly or of the Monitoring Body, which have to clearly state in writing the matters of the agenda and the purpose of the meeting.
- The decisions to accept new Members may be taken through email, without the need to convene a General Assembly. The decision shall be considered approved if, after three days of receiving the request for approval through email, the Members either approve or are silent. If a Member rejects accepting a new Member, then the Chairman of the General Assembly shall convene a regular General Assembly in accordance with the previous paragraphs.

8.1.1.5 Meeting

- The Members may participate in a General Assembly either physically or remotely via electronic meetings or conference calls, allowing all Members, participating in the meeting, to hear each other at all times and at the same time.
- The General Assembly may request experts to provide information on relevant topics or to attend meetings as invited guests to their deliberations.

8.1.1.6 Quorum and majorities

The General Assembly's resolutions may only be validly taken with a majority of the votes of the Members of the General Assembly. However, if there is not a quorum present when a meeting is first called, a simple majority of those present or represented at an adjourned meeting will suffice to approve the resolution.

The members of the General Assembly may pass unanimous decisions in writing or held a General Assembly without any prior formalities, provided always that all Members are present and express their agreement.

8.1.2 Code Steering Board

8.1.2.1 Composition

The Steering Board shall be comprised of a maximum of 13 (thirteen) Members, unless a bigger number of Members is decided by the General Assembly.

Each CSP Member of the Steering Board is entitled to one vote but may appoint up to three individual named persons to represent them at the Steering Board, and who may name a substitute if they are unable to participate in a Steering Board meeting. Each Member shall inform the Steering Board Chairman of who their representatives are. Individuals who represent their organisations in the Steering Board should have a proven expertise in the area of cloud computing and/or data protection and should also have a strong understanding of the cloud computing business models.

The Steering Board may pass a resolution to invite interested third parties to join the Steering Board with a view of strengthening the balanced representation of stakeholders interested in participating in the Code, from both the private and public sectors. In particular, it should be ensured, where possible, that the Steering Board includes representatives of:

- CSPs and Customers and their representative organisations (including representatives of the public and private sector);
- Academics or experts in data protection and cloud computing.

Should the need arise, in view of the future evolutions of the Code, the Steering Board may decide to appoint a drafting team of qualified experts to prepare amendments to the Code.

8.1.2.2 Powers

The Steering Board, directly or through any subcommittees it chooses to create, performs the following functions:

- Monitor changes in European Union data protection laws and propose changes to the Code for approval by the General Assembly. The Steering Board shall aim to propose relevant changes to the Code within three months of material changes in European Union data protection laws, taking into account the extent and complexity of the changes;

- In consultation with the Monitoring Body, define and propose templates and online forms for the submission of the declaration of adherence to the Monitoring Body;

- In consultation with the Monitoring Body, define and propose minimum requirements for the assessment of declarations of adherence by a Monitoring Body;

- Identify appropriate existing standards and certification schemes that can be used to confirm compliance with all or parts of the Code. The Steering Board will endeavour to take advantage, when appropriate, of existing third-party standards, schemes and audits which are relevant to (certain parts of) the Code;

- Define and propose more detailed guidelines for the application and interpretation of the Code taking into account any feedback of the Monitoring Body, where applicable, highlighting areas of frequently asked questions; such guidelines must not, however, never lower the level of data protection as provided by the present Code, and will, at all times, ensure compliance with the GDPR. Such guidelines must not materially change the Code. However, to adequately align with the competent supervisory such guidelines and any modification thereof shall be presented to the competent supervisory authority prior publication to enable the supervisory authority to request formal approval pursuant Article 40 GDPR, where considered necessary.

- Define and propose more specific modules to the Code, e.g. in relation to specific use cases, data types, service provisioning models, sectors or industries; such modules shall be submitted to the competent supervisory authority for approval pursuant Article 40 GDPR, without limiting any powers and deviating interpretation of supervisory authorities;

- Define, propose and update the Code Controls Catalogue, containing, among other, a dedicated control set and a map of existing standards and schemes;

- Adopt Compliance Marks that may be used by adhering Members;

- Appoint the Monitoring Body and withdraw or suspend the appointment in case of factual indications that the Monitoring Body no longer meets the requirements defined in this Code; A Competent Monitoring Body shall only be appointed by the Steering Board, after the Steering Board has determined that the Monitoring Body is capable of performing the functions referred in Section 7.2.2, and fulfils the following criteria to the satisfaction of the Steering Board: has established procedures which allow it to assess the eligibility of Members to declare their Cloud Services adherent to the Code; to monitor their CSPs and their adherent Cloud Services compliant with the Code's provisions, and to periodically review the Members operation if needed;

- Approve the Secretariat, selecting a suitable organisation to perform the Secretariat tasks on the basis of non-discriminatory and objective criteria;

- Discuss and submit for the approval of the General Assembly, membership fees, Supporters fees and, in consultation with the Monitoring Body, fees for declaration of adherences and their reviews, complaints fees, and any other fee that might be applicable;

- Propose, in consultation with the Monitoring Body, for the approval of the General Assembly, the allocation of a share of the annual membership fees, from Members that have their Cloud Services declared adherence, to safeguard the Monitoring Body legal minimum functionality and independence (Section 8.3.3);

- Propose, for the decision of the General Assembly, a list of sanction and remedies, to be applicable by the Monitoring Body, in case of an infringement of the Code, like suspension or exclusion from the Code, and the publication of such decisions taken by the Monitoring Body – notwithstanding and to no means limiting any legal obligation of the Monitoring Body to publish certain decisions;

- Adopt, for the decision of the General Assembly guidelines for sanctions and remedies, see Section 7.9.4;
- Work on particular issues and new developments impacting the Code, where necessary by establishing and proposing an annual work programme in consultation with the supervisory authorities, the European Data Protection Board and Commission and, where necessary, by developing proposals for the improvement of the governance.

8.1.2.3 Board

The Steering Board shall elect a Chairman from amongst its members, for a period of two years, with the possibility of renewing their mandate for any number of successive additional two-year terms.

The Members of the Steering Board shall be appointed in accordance with the following rules:

- If the total number of Members of the General Assembly is less than or equal to 13 (thirteen), each Member is entitled to appoint representatives to the Steering Board, as referred in Section 8.1.2.1;
- If the number of Members of the General Assembly exceeds 13 (thirteen), the Members shall make a decision, in a General Assembly, on whether to increase the number of Steering Board Members;
- The members of the Steering Board shall be elected through a unitary list, which shall contain the reference to the representatives appointed by each Member, to be proposed at the annual General meeting.
- Each Member agrees to vote in favour of the representatives, or any substitutes, proposed by the other Members.

8.1.2.4 Convene the Steering Board

Meetings of the Steering Board shall be held at regular intervals, as agreed by the Steering Board, and minutes of such meetings shall be prepared, as soon as practicable following such meetings by the Secretariat. Unless otherwise agreed, there shall be a minimum of 12 (twelve) meetings of the Steering Board in each year, to be held not more than two months apart.

Notice in writing of not less than five days, on first call, and one day on second call, shall be given to each Steering Board member of every proposed meeting of the Steering Board accompanied by an agenda specifying, in reasonable detail, the matters of the agenda.

Any member of the Steering Board shall have the right to call a meeting of the Steering Board at any time.

A meeting of the Steering Board may be convened on shorter notice provided that all the members of the Steering Board consent to such shorter notice.

8.1.2.5 Meeting and members' representatives

Each Member of the General Assembly shall procure that their respective appointees to the Steering Board attend each meeting of the Steering Board and they each shall use their best endeavours to procure that a quorum is present throughout each meeting of which due notice has been given.

The members may participate in the Steering Board either physically or remotely via electronic meetings or conference calls, allowing all representatives participating in the meeting to hear each other, at all times, and at the same time.

Provided that copies of all relevant documents are first sent to all the members of the Steering Board, a resolution of the Steering Board may also be taken without a meeting if it is agreed, in writing, by all members of the Steering Board.

Meetings of the Steering Board shall take place on the date and at the time designated in the notice of the meeting.

8.1.2.6 Quorum and Majorities

The quorum for all meetings, at first call, of the Steering Board shall be a simple majority of votes of all the members of the Steering Board. If a meeting is not quorate, it shall be adjourned to a date at least one day after the date of the first meeting. The quorum for a meeting adjourned shall be a simple majority of the members of the Steering Board present or represented.

8.1.2.7 Disputes amongst Members

The Steering Board shall develop appropriate policies to assure that interests are disclosed, and conflicts are avoided between Members. Mechanisms will include separation of duties, recusal or other policies undertaken by the Steering Board, and the possibility for the General Assembly to raise objections against individual Steering Board members. The Steering Board will also create an impartial mechanism to hear and decide on conflicts as well as appropriate appellate procedures related to decisions that impact organisations or competent bodies.

Without prejudice to the powers and capacity of the Monitoring Body, the Steering Board may propose to the General Assembly to temporarily or permanently suspend or revoke the membership status of any Member of the General Assembly due to infringements against the governance of this Code.

8.1.3 Code Supporter

Separately and without obtaining voting rights in the General Assembly, any interested individuals or organisations (including without limitation representatives of CSPs, user organisations, consumer protection bodies, civil rights groups, industry associations, government bodies or agencies, supervisory authorities, academia, or consultancy organisations) may apply for a membership in the General Assembly as Supporter. CSP's may not apply for Supporter Status.

All Supporters will be required to pay the annual Supporter membership fee, as set out by the General Assembly. Supporter status is automatically renewed for another year unless the Supporter does not express its request of termination 3 months prior to the end of their Supporter membership term. Supporters shall be published on the Code website and publicly declare their support to the principles of the Code.

8.1.4 Secretariat

The Secretariat performs the following functions:

- Maintain a public register of Cloud Services that are verified adherent;
- Maintain a public register of Code guidelines;
- At the request of the Chairman of the General Assembly, convene General Assembly meetings and request email decisions in accordance with the Code, prepare General Assembly meetings and draft minutes of the meetings;
- At the request of the Chairman of the Steering Board, convene Steering Board, meetings and request email decision in accordance with the Code, prepare meetings and draft minutes of the Steering Board;
- Promote the Code in Member States;
- Maintain the Code website;
- Perform other related functions at the request of the Steering Board.

8.2 Code and guidelines

A regular review of the Code and the Code guidelines to reflect legal, technological or operational changes and best practices, as well as experiences in the practical operation and application of the Code, shall take place when appropriate, and in any event at least every three years. Best practice initiatives shall be integrated and referenced where appropriate.

An additional review of the Code and the guidelines can be initiated at the request of two members of the Steering Board or the Monitoring Body.

The Steering Board may appoint a drafting team to conduct the review.

The General Assembly shall submit the revised Code for endorsement in accordance with Article 40 GDPR, whenever there has been a change to the Section 5, 6 or 7 of this Code. Adjustments to the Controls Catalogue shall be presented to the Supervisory Authority and, where considered necessary in consultation with such Supervisory Authority, those changes shall be submitted as revised Code as well. Comments from the supervisory authorities and the European Data Protection Board should be incorporated as appropriate, approved by the General Assembly and published.

For the avoidance of doubt: to the extent the Code allows for further particularization by guidelines or supporting documents, such guidelines and supporting documents must not undermine or materially affect neither the provisions and safeguards of the Code, nor the powers of the Monitoring Body. Such guidelines and supporting documents shall always be brought to the attention of the competent supervisory authority.

8.3 Finances

8.3.1 General

The costs for the Secretariat (see Section 8.1.4) and the Monitoring Body (see Section 7.2) should be covered by fees raised by its Members and Supporters.

All costs of the Secretariat and the Monitoring Body and fees are publicly available.

8.3.2 Secretariat

The General Assembly shall decide in the annual General Assembly meeting the adequate share of the membership fees to cover the Secretariat administration costs.

8.3.3 Monitoring Body

Fees that Members pay to obtain the approval of a declaration of adherence by the Monitoring Body shall be allocated to cover the operating costs of the Monitoring Body. The fees apply regardless of the outcome of the declaration of adherence process.

Additionally, the Monitoring Body shall receive an adequate share of Members annual membership fees to safeguard the Monitoring Body's legal minimum functionality and independence, including its complaints mechanism and constant monitoring.

8.3.4 Complaints

Complaints may be subject to fees, which shall be cost-based and approved by the General Assembly. Detailed provisions are governed in Section 7.8.3 of the Code.

9 ANNEX A – Controls Catalogue

– CONFIDENTIAL UNTIL OFFICIAL APPROVAL OF THE CODE –

EU Cloud Code of Conduct

Annex A

Controls Catalogue

Version:	2.11
Publication Date:	December 2020
Website:	https://eucoc.cloud

0 Contents

1 Introduction

In order to ensure that the Monitoring Body and supervisory authorities can verify that requirements of this Code are met by the Cloud Services declared adherent, requirements of this Code have been translated into controls. Each control is given a unique identifier (Control-ID) of the pattern Section.Subsection.Letter, e.g. 5.1.A.

For each Control, where appropriate, there is also a guidance ("Control Guidance"). This Control Guidance is a selection of best practices on how the Control can be implemented by CSPs declaring a Cloud Service adherent to this Code. The Control Guidance is not mandatory, however, if CSPs implement alternative measures, they cannot be less protective than those being provided by the Control Guidance.

For the avoidance of doubt: Wherever the Code and this Controls Catalogue makes use of the terms "shall" and "must", a CSP is obliged to implement the respective provision in order to be compliant with the Code; even if the respective provision is not translated directly into a Control. Wherever the Controls Catalogue makes use of the terms "should", "may" or "can", examples and recommendations are introduced. It is worth noting that even in cases of non-binding provisions indicated by such terms, the examples and recommendations establish good practices and if the CSP chooses an alternative implementation, in order to be compliant with the Code, the respective implementation must be as effective and no less protective than the given guidance. In case binding requirements of the Controls Catalogue and any part of the Code may be conflicting in order to reach compliance, the Code prevails.

2 Controls of Section 5, Control Guidance and Referencing with International Standards

Controls of Section 5 have been referenced to internationally recognized standards where relevant, including ISO/IEC 27001:2013, ISO/IEC 27018:2019, ISO/IEC 27701:2019, SOC 2, and Cloud Computing Compliance Controls Catalog (“C5”), in order to provide CSPs with best practices of similar areas which might act as reference and starting point when implementing specific data protection related measures.

Please note: GDPR mapping is considered a starting point which GDPR provisions relate to the Control; GDPR mapping is not intended to provide an exhaustive and binding reference of which GDPR provision is being thoroughly particualrized. Consequently, compliance with the respective Controls does not necessarily relate to an exhaustive compliance with the provided GDPR provisions.

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[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. [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.A] The Cloud Services Agreement should cover relevant terms related to the delivery of the Cloud Service. The CSP should incorporate at least the same level of rights and protections afforded by the GDPR in the Cloud Services Agreement. *Relevant terms meaning all terms covering the processing of Customers Personal Data by the CSP* [5.1.B] As part of the Cloud Services Agreement the CSP should commit declared Cloud Services to compliance with relevant Data Protection regulations, including GDPR and this Code *Relevant Data Protection regulations - means any National EEA Data Protection Implementation of GDPR*	Art. 28	A.18.1 - Compliance with legal and contractual requirements	18.1 - Compliance with legal and contractual requirements	18.1 - Compliance with legal and contractual requirements A.10.11 Contract measures	B.8.2.1 Customer agreement	A1.1 A1.2 A1.3 C1.1 C1.2 PI1.1 PI1.2 PI1.3 PI-1.4 PI1.5 P1.1 - P8.1	COM-01 Identification of applicable legal, contractual and data protection requirements.
[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 re-quirements of the Code to	[5.1.C] The Cloud Service Agreement should define the roles and responsibilities of CSP and Customer with respect to security measures. The requirement is for the CSP and the Customer to agree the roles and responsibilities for the security measures. The approach to this process should be flexible to accommodate the various types of contractual relations between CSPs and their customers. [5.1.D] CSP should have procedures in place for addressing individual inquiries, complaints and disputes around non-compliance to the Code.	Art. 28, Art. 28.9,Art. 32	A.18.1.1 - Identification of applicable legislation and contractual requirements A.5.1.1 - Policies for information security A 6.1.1 Information security roles and responsibilities	5.1.1 Policies for information security 6.1.1 Information security roles and responsibilities	5.1.1 Policies for information security A.10.11 Contract measure 6.1.1 Information security roles and responsibilities	B.8.2.1 Customer agreement B.8.3.1 Obligations to PII principals	CC2.2 CC2.3 CC1.1 CC2.2 CC2.3 P8.1	COM-01 Identification of applicable legal, contractual and data protection requirements. DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
adequately deal with related Customer inquiries [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.	*procedures*" in this context should cover elements like: ■ the identification of inquiries, complaints and dispute ■ appropriate communication channels ■ where Customer insists indicating the possibility that Customer may file the issue concerned to the Monitoring Body for review ■ resolution of issue [5.1.E] If Customer is aware of a CSPs adherence to the Code and may easily access the Code's website and public register, each Customer will automatically be prpvided with transparent and easy accessible information to being enabled to file a complaint and how to do so. *CSP must appoint a point of contact to address Code related questions.*							OIS-02 Strategic targets regarding information security and responsibility of the top management
[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.F] The Cloud Service Agreement should cover the personal data processing activities conducted by the CSP on behalf of the Customer. These activities should take into account: ■ security, ■ confidentiality, ■ processing integrity, ■ availability, and ■ data protection of the Customer Personal Data. [5.1.G] Terms related to the use of subprocessors by the CSP to deliver the Cloud Service should be defined by the Cloud Services Agreement subject to the nature and purpose of processing. For further details on requirements and guidance regarding the engagement of subprocessors refer to Controls [5.3.A] to [5.3.F].	Art. 28.2, Art. 28.3, Art. 28.4, Art. 29	N/A	N/A	A.2.1 Public cloud PII processor's purpose	B.8.2.1 Customer agreement B.8.2.2 Organization's purposes B.8.2.6 Records related to processing PII B.8.5.7 Engagement of a subcontractor to process PII	CC3.1	COM-01 Identification of applicable legal, contractual and data protection requirements. UP-02 Jurisdiction and data storage, processing and backup locations
[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 subprocessors.	[5.1.H] The terms related to the processing activities by the CSP and any other third-party engaged by the CSP or Customer should be formally documented in the Cloud Services Agreement. The processing activities should be defined in a manner that considering e.g. an average Customer who may consult experts may understand it, taking into account the nature of the processing and Cloud Service.	Art. 28	N/A	N/A	A.2.1 Public cloud PII processor's purpose A.2.2 Public cloud PII processor's commercial use	B.8.2.1 Customer agreement B.8.2.2 Organization's purposes B.8.2.6 Records related to processing PII	CC3.1	COM-01 Identification of applicable legal, contractual and data protection requirements. UP-02 Jurisdiction and data storage, processing and backup locations

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[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.	[5.2.A] The Cloud Service Agreement should define the roles and responsibilities of CSP and Customer with respect to the processing of personal information. The responsibilities should include CSP obligation to assist Customer to comply with the GDPR taking account the nature of the Processing and the information available to the CSP. *the nature of the Processing*” recognises the fact that there are/may be a variety data processing activities carried out by the CSP on behalf of the Customer. For a better understanding refer to the example below. *the information available to the CSP*” recognises that the CSP in all instances may not have access to the Customer Personal Data. **Example** Some CSPs may provide Cloud Services which do not entitle the CSP access to Customer Personal Data, either technically or by way of contractual restrictions. In the situation where the CSP can access Customer Personal Data and the Customer cannot, the CSP should assist the Customer.	Art. 28	A.18.1 - Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.2.1 Public cloud PII processor's purpose	B.8.2.2 Organization's purposes B.8.2.5 Customer obligations B.8.2.6 Records related to processing PII B.8.3.1 Obligations to PII principals 6.15.1 Compliance with legal and contractual requirements	CC3.1 CC2.2 CC2.3 CC1.1 CC3.1 CC2.2 CC2.3 CC9.2 P5.1	COM-01 Identification of applicable legal, contractual and data protection requirements. KOS-08 Confidentiality agreement OIS-01 Information security management system (ISMS) OIS-02 Strategic targets regarding information security and responsibility of the top management
[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] CSP should have procedures in place to ensure that CSP makes available to the Customer necessary information relating to the processing of Customers' Personal Data, to assist the Customer's compliance obligations under the GDPR. **Example** The CSP may make available to the Customer: ■ Third party attestations ■ Information of Technical and Organizational measure to protect Customer Personal Data ■ Communications channels ■ Options to audit							
[5.2.C] CSP shall communicate mechanisms to the Customer how to access the information of 5.2.B.	[5.2.C] CSP should provide mechanisms to the Customer which will allow access to the information referred in 5.2.B **Example** Applicable mechanisms may include: ■ Customer Portal ■ Customer communication channels ■ Virtual tours ■ Published resources.							

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[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] CSP should have procedures in place to ensure that Customer Personal Data shall be processed according to Customers documented instructions. The Cloud Services Agreement shall determine the scope of the Customers instructions for the processing of the Customers Personal Data. *scope of the Customers instructions”* here refers to the exact definition of what the Customers processing instructions to the CSP cover, in terms of the service being provided by the CSP to the Customer. In this context procedures” should cover aspects like: ■ format of acceptable Instructions from the Customer to the CSP ■ 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. [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.	[5.2.E] Operational mechnanisms and schedules may entail both mechanisms and procedures. Those refer to the functionality which the CSP provides to the Customer to enable the Customer to delete Customer Personal Data from the Cloud Service. **Example** Subject to the nature of the Cloud Service, the CSP may provide: ■ deletions schedule functionality ■ deletion schedule notification ■ enhancements and features to enable deletion of data Functionality may provide, that the above examples can be triggered manually or automatically, via the Cloud Service itself, a Customer Portal or any other Communication Channel. Whilst expected that Customers will be enabled to individually maintain their retention policies, CSP may alternatively or additionally provide a general, fully automatic deletion schedule for Customer Personal Data. [5.2.F] Where applicable, based on the nature of the processing activities and the Service provided by the CSP, CSP shall train its personnel on such retention policies and schedules and shall undertake oversight and monitoring to ensure that such schedules are followed. *Where applicable”* - here is a reference to the fact that [5.2.E] provides two dimensions. Where CSP provides	Art. 5 (e), Art. 28.3 (g), Recital 39	A12.3.1 - Information Backup A 7.2.2 -Information Security Awareness, education and training	12.3.1 Information backup 7.2.2 -Information Security Awareness, education and training	A.9.3 PII return, transfer and disposal A.9.2 Retention period for administrative security policies and guidelines	B.8.2.6 Records related to processing PII B.8.4.2 Return, transfer or disposal of PII 6.4.2.2 Information security & privacy awareness, education and training	CC3.1 A1.2 A1.3 PI1.1 A1.2 A1.3 P4.2	COM-01 Identification of applicable legal, contractual and data protection requirements. OIS-01 Information security management system (ISMS) RB-06 Data backup and restoration – concept RB-07 Data backup and restoration – monitoring

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[5.2.G] CSP shall communicate its standard retention policies and schedules regarding Customer Personal Data to its Customers.	functionality to enable Customers to individually matain their retention policies, CSP has no reason and capability to train its personnel on such policies and hence may not monitor them. Where CSP, however, provides general retention schedules for its service CSP needs to ensure compliance with such policies, e.g. by training its personnel on such retention policies and schedules accordingly and establish appropriate monitoring. *the nature of the Processing*” here means that there are a variety data processing activities carried out by the CSP on behalf of the Customer. [5.2.G] Where applicable, based on the nature of the processing activities and the Service provided by the CSP, CSP should have a mechanism to communicate its standard retention policies and schedules to its Customers. *Where applicable*” - here is a reference to the fact that there may be instances where CSP leaves retention solely to the discretion of the Customer							
[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.A] CSP should have mechanisms in place to ensure that written authorization of the Customer is in place, prior to engaging subprocessors, in the processing of Customer Personal Data. *mechanisms*” here means a recorded means of ensuring that written authorisation is in place. **Example** This can be achieved by authorisation of the Customer, per Processor, or by way of a general pre-authorization between the CSP and the Customer. [5.3.B] Where a CSPs subprocessor is rejected by the Customer, the CSP shall follow the agreed upon procedures in place, in the Cloud Service Agreement. The CSP should provide alternative options such as a change of subprocessor or an option to exercise termination rights. If and to the extent, the CSP explicitly reserves the possibility by according provisions within the Cloud Service Agreement to apply any changes to subprocessors with limited, in exceptional and emergency situations even without any prior notice to the Customer due to measures beyond CSP's reasonable control, e.g. damage of subprocessor facilities, subprocessor bankruptcy, or any force majeure, this should not be considered as negatively	Art. 28.2, Art. 28.3 (d), Art. 28.4	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.7.1 Disclosure of sub-contracted PII processing	B 8.5.6 Disclosure of subcontractors used to process PII B 8.5.7 Engagement of a subcontractor to process PII B 8.5.8 Change of subcontractor to process PII	N/A	DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	influencing the Customer's measures to prevent the respective processing. *Reasonable prior notification*”: To evaluate whether the notification period has been reasonable, it should also be taken into account, whether the Customer is able to perform its rights under the Cloud Service Agreement after reasonably considering its alternatives and consequences, taking into account the nature of the Cloud Service and processing. **Example** Having provided the Customer with advance notice of the intention to use a particular subprocessor, the CSP, where practical (and not contrary to the feasibility of the Cloud Service), may provide an alternative subprocessor for the Customer, should the Customer object to the use of the suggested subprocessor. Alternatively, the CSP may allow the Customer to off board from the Cloud Service provided by the CSP, subject to the terms of the Cloud Services Agreement.							
[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.	[5.3.C] CSP should have procedures in place regarding subprocessor management which enable the CSP to evaluate any subprocessors which the CSP will engage in Customer Personal Data processing activities. This should be subject to the terms of the Cloud Services Agreement. **Example**: Such procedures covering subprocessor management should take account of: ■ the nature of the personal data processing activities of the subprocessor ■ the standing of the subprocessor, in terms of regulatory compliance ■ the geographical reach of the subprocessor in terms of personal data processing ■ technical and organisational measures in place ■ etc [5.3.D] CSP shall have procedures in place to ensure that the same data protection obligations as set out in the CSA with the Customer and that the subprocessor has technical and organisational controls in place that are no less protective than those of the CSP and that align with the CSP's obligation to the Customer.	Art. 28.4	A.18.1 Compliance with legal and contractual requirements A.13.2.2 - Agreements on information transfer: A.15.1 Information security in supplier relationships A.15.2 Supplier service delivery management	18.1 Compliance with legal and contractual requirements 15.1.2 Addressing security within supplier agreements 15.1.3 Information and communication technology supply chain	A.10.12 Sub-contracted PII processing:	B 8.5.7 Engagement of a subcontractor to process PII 6.12.1 Information security & privacy in supplier relationships B.8.2.6 Records related to processing PII	CC3.1 CC1.4 CC2.3 CC3.2 CC3.4 CC9.2 P6.4 P6.5	COM-01 Identification of applicable legal, contractual and data protection requirements. DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	Those procedures should entail: ▪ where a CSP engages another processor for carrying out specific processing activities on behalf of the Customer, the same data protection obligations as set out in the Cloud Service Agreement or other legal act between the Customer and CSP shall be imposed on that subprocessor by way of a contract. ▪ such Cloud Service Agreement or other legal act shall in particular provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Code, the Cloud Service Agreement between CSP and Customer and the GDPR. ▪ due diligence of the subprocessor to check the Technical and Organisational measures that it has in place ▪ From time to time carry out due diligence to check the compliance with terms of the subprocessor agreement Requirement is to ensure that the subprocessor contracts provide no less protection than those between CSP and the Customer – this is e.g. achieved through the contractual agreements. *"Time to time"* should be understood as, periodically taking into account the associated risks of the subprocessing activity. The CSP should conduct an assessment of the data protection practices and verify that those are align with relevant Cloud Service Agreement the CSP provides to its Customers.							
[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.	[5.3.E] Customer should be enabled to take an informed decisions prior entering into any binding Cloud Service Agreements. Additionally, Customer needs certain information to assess whether CSP will comply with its obligation to prior notify about changes of applicable jurisdictions or changes of applicable subprocessors. However, the Code aknowledges that certain information may also be confidential or even may create security risks if being communicated publicly. Thus, the CSP may – up to its discretion – decide to limit its information communicated prior entering into a Cloud Service Agreement to the what is necessary for an informed decisions and / or only provide such information subject to a non-disclosure agreement.							

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[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] CSP should have mechanisms in place to provide lists of subprocessors to the Customer that process Customer Personal Data, and where a general pre-authorization is in place CSP shall ensure that any change (addition or replacement) to the list is communicated to the Customer in advance. *mechanisms*” here means that the CSP should have an established way of communicating with the Customer in advance of onboarding subprocessors **Example**: CSP should communicate the existence of and access to the list in the Cloud Service Agreement. The list may be accessible in a ■ public website, ■ contract, or ■ Customer Portal relevant for the Cloud Service. CSP should notify Customer about any changes of subprocessors by available mechanisms, e.g.: ■ email ■ public website ■ Customer Portal The provisions of ISO 27018 A7.1 may serve as a non-compulsory guideline.	Art. 28	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.7.1 Disclosure of sub-contracted PII processing:	B 8.5.8 Change of subcontractor to process PII 6.12.2 Supplier service delivery management	CC1.3 CC2.3 CC3.1 CC3.4	DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider
[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..	[5.3.G] The CSP may agree upon certain jurisdictions both explicitly within the CSA or by any other direct or indirect but binding reference to applicable jurisdiction at the time of agreement, e.g. by reference to a list of subprocessors. A limitation of aplicable jurisdictions should not be considered cases, where the CSA explicitly states that Customer Personal Data may be processed wordwide and the list of subprocessors has only been provided for informational purposes. Where the CSA explicitly limits the applicable jurisdictions, any change is considered lawful only, if the Customer authorizes such change. For the ease of performance of contract the CSP may however request a general authorization within the CSA, provided that such changes will be subject to a prior notification. CSP should notify Customer about any changes of of applicable jurisdictions to a subprocessor engaged by available mechanisms, e.g.: ■ email		A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.7.1 Disclosure of sub-contracted PII processing:	B.8.5.1 Basis for PII transfer between jurisdictions 6.12.2 Supplier service delivery management	CC1.3 CC2.3 CC3.1 CC3.4	DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	■ public website ■ Customer Portal The provisions of ISO 27018 A7.1 may serve as a non-compulsory guideline.							
[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] Where transferring Customer Personal Data, the CSP's shall utilize the appropriate mechanisms permitted by law. The CSP should have mechanisms in place to ensure that protective controls are in place to ensure the security of data transfer.	Art. 28.3 (a), Art. 44, Art. 45, Art. 46, Art. 47	A.18.1 Compliance with legal and contractual requirements A.13.2 - Information Transfer	18.1 Compliance with legal and contractual requirements 13.2 - Information Transfer	18.1 Compliance with legal and contractual requirements A.11.1 Geographical location of PII 13.2 - Information Transfer	B.8.5 PII sharing, transfer and disclosure B.8.5.1 Basis for PII transfer between jurisdictions B.8.5.2 Countries and international organizations to which PII can be transferred 6.10.2.2 Agreements for information transfer	CC6.7 CC2.2	UP-02 Jurisdiction and data storage, processing and backup locations DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider
[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] CSP should have procedures in place that ensure that transfers of Customer Personal Data to third countries outside the EEA are subject to appropriate safeguards (please refer to Control [5.4.E]) and to the extent and modalities provided by the Cloud Service Agreement. For the avoidance of doubt: If and to the extent a Cloud Service Agreement allows for additional instructions related to third country transfers, any legitimate instruction shall also considered as reflected by respectively 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.C] CSP should have procedures in place that ensure that transfers of data to a third country outside the EEA meet the established transfer requirements. **Example**: Appropriate safeguards may be reached e.g. by ■ Binding Corporate Rules in accordance with Article 47 GDPR; ■ Standard data protection clauses approved by the EU Commission in accordance with Article 93.2 GDPR; ■ An approved code of conduct pursuant to Article 40 GDPR, together with binding and enforceable commitments of the processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; ■ An approved certification mechanism pursuant to Article 42 GDPR, together with binding and enforceable commitments of the processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.							

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[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. [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.	[5.4.D] CSP shall have procedures in place to determine whether the destination of a data transfer is subject to an adequacy decision of the Commission. **Example** The CSP should refer to the list of Adequacy decisions here: https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en [5.4.E] CSP should have established procedures that note, where the destination of a data transfer is to a country that is outside the European Economic Area, and on which safeguard of Chapter V (e.g. adequacy decision, binding corporate rules) it is based. CSP should have procedures in place to prevent the transfer of Customer Personal Data to a destination that is outside the European Economic Area and is not subject to the adequacy finding by the European Commission, where appropriate safeguards are not in place. **Example**: Such mechanisms should include: ▪ safeguards that data transfers that were solely subject to an adequacy decision can be easily identified ▪ ability to terminate if status of adequacy changes or made subject to any alternative safeguard in case the adequacy decisions is declared void.							
[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] Where applicable, 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. In this scenario the CSP should have Policies and Procedures in place to comply with the terms of Article 27 GDPR. *Where applicable"* - here is a reference to the fact that there are instances where the CSP is established in a Member state of the EU and is in scope for GDPR.	Art. 27	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	6.15.1 Compliance with legal and contractual requirements	CC2.3	COM-01 Identification of applicable legal, contractual and data protection requirements. UP-02 Jurisdiction and data storage, processing and backup locations
[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.A] CSP should provide mechanisms to make available to the Customer all information necessary to demonstrate compliance with the obligations of the Customer under the Code and GDPR.	Art. 28.3 (h), Art. 28.3 (b), Art. 28.4, Art. 32	A.18.1 Compliance with legal and contractual requirements A.18.2 Information	18.1 Compliance with legal and contractual requirements 14.1.1 Information	18.1 Compliance with legal and contractual requirements A.18.2 Information	B.8.2.1 Customer agreement B.8.2.5 Customer obligations	CC4.1 CC3.1 CC3.2 CC4.2 CC8.1	UP-04 Certifications COM-02 Planning independent, external audits

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	Example: Where applicable, independent third party audit reports and certifications can be made available in a centralized repository, for Customers. Additionally, material for Customers such as Whitepapers and Product Documentation can be made available via Customer Portals.		security reviews A.12.7 Information systems audit considerations	security requirements analysis and specification A.18.2 Information security reviews	security reviews	B.8.2.6 Records related to processing PII 6.15.1 Compliance with legal and contractual requirements 6.15.2 Information security & privacy reviews	CC9.2 P8.1	COM-03 Carrying out independent, external audits OIS-01 Information security management system (ISMS)
[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] Upon request, the CSP should provide the Customer with the most recent certifications or summary audit reports, which the CSP has procured to regularly test, assess and evaluate the effectiveness of its security measures. Where a subprocessor is acting on behalf of the CSP and has access to the Customer Personal Data, the CSP should provide an overview of the service provided by the applicable subprocessor and demonstrate, (for the applicable control set) that the subprocessor has no less protective security controls in place, to meet the obligations of the CSP under this code and GDPR.							
[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] CSP should have appropriate policies/procedures regarding independent third party audits and communicated to the Customer. For a better understanding, please refer also to Control [5.5.D]. When drafting its procedures CSP shall take into account: ■ ensuring confidentiality and security of the premises; ■ minimising risk of disruption to CSP's business and other Customers; ■ minimising risk of data breaches caused by the audits; ■ ensuring conformity with the CSP's practices, policies and legal obligations; ■ ensuring compliance with any agreements, rights or legal obligations of other Customers or their data subjects; ■ requiring the Customer to provide written notice reasonably in advance of the proposed audit date; ■ setting forth a defined scope for a mutually agreed audit plan.							
[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	[5.5.D] If the CSP is requested to provide further evidence which is not provided by the above mechanisms, the CSP can request the Customer to bear the cost of any such further assistance.							

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
requirements of the GDPR, where this evidence is not provided by other means.	Independent third party reports and certifications conducted against recognized international standards provide an efficient and reliable way for users to fulfil their statutory obligation to review Cloud Services. In cases where such reports are not available and/or do not fully address the obligations of the Customer, the CSP should allow for an audit by the Customer based upon defined CSP's customer audit procedures. For example, the procedures will describe key elements of the audit program such as: ■ Period of advance notice ■ Fees charged by the CSP for assistance, or criteria to determine such fees ■ Security and confidentiality restrictions These procedures should be defined by the CSP as part of the Cloud Service Agreement or separate audit agreement and should specify the terms for audit. Since on-site audits always involve the risk of disrupting the business processes of the CSP and its clients, Customer audit planning and execution shall be as terms of the contractual agreements. The CSP should ensure that any subprocessor is subject to mechanisms that are no less protective as laid down in this section of this Code with regards to subprocessors' obligations to enable CSP to assess whether the processing activities are in compliance with its obligations of this Section under the Code, and under GDPR as a processor. Equivalent mechanisms e.g. may be that ■ Customer may request documentation of compliance, e.g. by certifications or audits, for all subprocessors in the chain. CSP may in those cases gather the information on request in a timely manner ■ Customer may request - subject to appropriate NDAs - documentation of compliance by third party reports Aforementioned aspects may be set-up as stages; i.e. Customer may only request further details to the extent he can substantially argue that the provided details are not sufficient for his needs to evaluate his own or CSPs GDPR compliance.							
[5.5.E] If and to the extent Customer will have to bear any costs related to the per-	[5.5.E] There may be several models how costs arising for a CSP will be covered. Whilst some CSP may include a							

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
formance of its audit right, such costs must not be prohibitive or excessive.	share of such costs into general service fees, and thus charge each Customer regardless whether such Customer eventually performs its rights, CSP may also implement models where Customer performing their audit right will be charged accordingly. Especially where CSP opts for the latter, such charges must not be prohibitive. Costs shall not be considered probitive, e.g. where ▪ each party is bearing its own costs; i.e. Customer mandanted auditor and any related costs (travel, allowances, etc) are beared by Customer and any costs resulting from supporting personnell provided by CSP will be beared by CSP, or ▪ the CSP requires Customer to bear the actual costs of any personnel supporting; assisting or attending the audit – e.g. to safeguard security and confidentiality of processing – dprovided that the costs can be reasoned. CSP may charge for administrative burdens, e.g. resulting from efforts in providing (sanitized) copies of reports and documents to Customer to the extent they are not made publicly available; in such cases the costs should be limited to the administrative costs that results from such burdens; this can be done by means of a lump sum provided that such lump sum is not excessive. Also this applies for other measures, such as workshops or provisions of resources – e.g. additional bandwidth, dedicated testing environments – as necessary for particular testing, such as pen-testing.							
[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.	[5.5.F] The Code allows for a high degree of flexibility related to Customer Audits, which may be – depending on the individual necessities and circumstances - anything from an assessment of documents provided, workshops or to a physical examination of CSP premises, where such examination is capable to provide any added value. At the same time, the Code requires several safeguards to ensure that Customer are not effectively hindered in performing its right pursuant Article 28.3 (h) GDPR. It is expected that CSP is prepared for any Customer requests to react adequately and in due time. Also to enable effective monitoring existing procedures and provisions are needed. Customer Audit Provisions, though, must not be a dedicated agreement, but they can also take the form of an annexes or exhibits to other documents or may cumulate to a procedural reference.							

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[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.	The Cloud Service Agreement may specify Customers rights in case CSP has acted unlawfully, namingly against or outside lawful instructions of the Customer. This may include that personnel and / or contractors (such as external lawyers) are made aware of this section, e.g. by training.	Chapter VIII	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.1.1 Obligation to co-operate regarding PII principals' rights	B.8.2.1 Customer agreement B.8.2.4 Infringing Instruction 6.15.1 Compliance with legal and contractual requirements	CC3.1 CC7.4	COM-01 Identification of applicable legal, contractual and data protection requirements. UP-02 Jurisdiction and data storage, processing and backup locations
[5.7.A] CSP shall establish documented procedures to assist the Customer for fulfilling data subject access requests.	[5.7.A] CSP should enable Customer to fully address data subject access requests in a timely manner. CSP should document the methods available to the Customer and whether these methods fully enable Customers to address data subject access requests. In the case where a CSP has not fully enabled Customer to address data subject access requests, the CSP should provide assistance to the Customer to fully address data subject requests. CSP's procedures should cover all necessary aspects to provide response to Customer in due time, including ▪ internal technical and organisational measures to locate and extract relevant data, ▪ defined data formats and communication channels with Customer to make data available. Where the Code requires reasonable" assistance, reasonability shall take into account whether such assistance is actually possible for CSP. **Example** Some CSPs may provide Cloud Services which do not entitle the CSP access to Customer Personal Data, either technically or by way of contractual restrictions. In the situation where the CSP can access Customer Personal Data and the Customer cannot, the CSP should assist the Customer.Reasonability may also relate to the efforts required by CSP; e.g. if and to the extent Customer is already fully enabled to response to data subject access requests, CSP's reasonable assistance may be to provide Customer e.g. with supporting documentations, guidebooks, wikis or communication channels.	Art. 28.3 (e)	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.1.1 Obligation to co-operate regarding PII principal's' rights	B.8.2.5 Customer obligations B.8.3.1 Obligations to PII principals	P5.1 CC3.1 CC2.2 CC2.3	COM-01 Identification of applicable legal, contractual and data protection requirements.
[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] CSP shall e.g. ▪ provide the Customer with the ability for the Customer to gather, modify or delete Customer Personal Data itself, via the Cloud Services provided by the CSP or through							

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	standardised interactive interfaces or Customer Portals made available by the CSP, and/or ■ provide additional reasonable assistance in gathering, modifying or deleting Customer Personal Data, to the extent Customer Personal Data is not accessible to the Customer and/or cannot be modified or deleted by the Customer. ■ make available to Customer communication channels by which the Customer may address its questions and requests for cooperation regarding data subject rights requests. Where the CSP provides communication channels, the CSP should establish proceodures enabling the CSP to provide additional reasonable assistance in gathering, modifying or deleting the data, to the extent such data is not accessible to the Customer.							
[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] Communication channels should be designed to sufficiently enable Customer to submit its questions or requests, with no limitation on ■ characters, ■ formatting, and ■ attachments. Customer may be made available the respective communication channels either via ■ the Cloud Services Agreement, ■ the Cloud Service provided, ■ a public website, or ■ a Customer Portal. Whenever changes apply, CSP should provide updates to the Customer. At a minimum, CSP ensures that Customer may address its questions and requests to the Data Protection Point of Contact.	Art. 28.3 (e), Art. 28.3 (f), Art. 28.3 (h)	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.1.1 Obligation to cooperate regarding PII principal's' rights	B.8.2.1 Customer agreement 6.15.1 Compliance with legal and contractual requirements	P8.1 CC2.3	DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider
[5.7.D] CSP shall establish documented procedures to assist Customer with Data Protection Impact Assessment.	[5.7.D] CSP should have procedures in place which enable assistance to be provided to the Customer regarding Data Protection Impact Assessments. **Example**: As determined by the Cloud Services Agreement, the CSP may make available to the Customer ■ details of subprocessors, ■ applicable reports and documentation related to international recognized certification or audit schemes, ■ information around relevant technical and	Art. 28.3 (f), Art. 28.3 (b), Art. 30	A.18.1 Compliance with legal and contractual requirements A.12.6.1 Management of technical vulnerabilities	18.1 Compliance with legal and contractual requirements 12.6.1 Management of technical vulnerabilities	18.1 Compliance with legal and contractual requirements 12.6.1 Management of technical vulnerabilities	B.8.2.1 Customer agreement B.8.2.5. Customer obligations B.8.2.6 Records related to processing PII 6.15.2.3 Technical compliance review	CC2.3 CC3.1 CC3.2 CC4.2	DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider OIS-01 Information security management system (ISMS)

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[5.7.E] CSP shall establish documented procedures to safeguard 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.	organisational measures. Provide documentation in relation to how the Cloud Service protects Customer Personal Data. [5.7.E] CSP should have procedures in place to categorise the information which may be shared with Customers, to assist the Customer with a Data Protection Impact Assessment. **Example**: ■ where appropriate confidential information may only be provided subject to a non-disclosure agreement ■ confidential information may not be provided to Customer at all, as this information can be used to determine relevant vectors to attack CSPs service ■ Publicly available documentation Where CSP cannot provide information, not even subject to a confidentiality agreement, CSP should assist Customer by other means to the extent possible. Please also refer to the Guidance for Controls in Section 5.5 regarding the means.							
[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] CSP should have established processes in place to 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. For the avoidance of doubt: During the course of the provision of Cloud Services retrieval of Customer Personal Data technically equals the retrieval of a copy of Customer Personal. To the extent Customer entrusted Customer Personal Data by entrusting dedicated hardware, such as hard drives, retrieval of such dedicated hardware automatically, by technical means, results into incapacity of service provision by CSP; though there may be cases where it seems sensible such hardware retrievals are expected to happen in the course of terminating the Cloud Service Agreement. **Example**: The CSP may communicate the main characteristics of	Art. 28.3 (e), Art. 28.3 (g)	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.9.3 PII return, transfer and disposal	B.8.4.2 Return, transfer or disposal of PII B.8.4.3 PII transmission Controls	C1.2	PI-01 Use of public APIs and industry standards PI-02 Export of data PI-03 Policy for the portability and interoperability PI-04 Secure data import and export PI-05 Secure deletion of data

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	the available information in the Cloud Service Agreement or any other official documentation or service description. Main characteristics of the data may include: a) processes b) technical requirements, i.e. i) available data formats ii) transfer mechanisms iii) transfer characteristics iv) required configuration at the Customer's side c) timeframes d) any charges that apply							
[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.	[5.8.A] CSP shall maintain up-to-date and accurate record of processing activities carried out on behalf of the Customer in accordance with the CSPs obligations and with Article 30,2 GDPR. **Example**: The record of processing activities should at least contain: - The name and contact details of each Customer (as provided by the Customer) on behalf of which the CSP is acting, - The categories of processing carried out on behalf of the Customer, - The list of subprocessors who carry out certain activities on the behalf of the CSP, - Where applicable, transfers of Customer Personal Data to a third country and the underlying documentation of suitable legal safeguards to secure the transfer. [5.8.B] CSP should 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. **Example:** Customer communications channels can be used to ensure that the Customer keeps the CSP up-to-date with any relevant changes. The CSP may provide self-service mechanisms by which the Customer may update its list of controllers.	Art. 30.2, Art. 30.3	A.18.1 Compliance with legal and contractual requirements A 12.4 Logging and Monitoring A 9 Access control	18.1 Compliance with legal and contractual requirements 12.4 Logging and Monitoring 9 Access control	18.1 Compliance with legal and contractual requirements 12.4 Logging and Monitoring 9 Access control	B.8.2.1 Customer agreement B.8.2.6 Records related to processing PII	CC7.2 Pi1.3 P6.2 CC2.2 CC2.3	DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider
[5.9.A] CSP shall designate Data Protection Point of Contact with competencies according to Chapter IV, Section 4 GDPR.	[5.9.A] As applicable to Chapter IV, Section 4 GDPR, the CSP should appoint a Data Protection Officer. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 or any update thereof may	Art. 37, Art. 37.7	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	6.3.1.1 Information security & privacy roles and responsibilities	CC1.1 CC2.2 CC2.3 CC3.1	OIS-03 Authorities and responsibilities in the framework of information security

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[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 data subjects.	serve as guideline with regards to the competencies of the Data Protection Point of Contact. [5.9.B] The contact data of Data Protection Point of Contact shall be communicated and available to the Customer and – where required by GDPR – competent supervisory authorities, and upon request data subjects. **Example**: Where relevant the CSP will communicate Data Protection Officer details to the supervisory authorities, in terms of registration. The CSP will communicate Data Protection Point of Contact details to Customers through relevant interaction channels, including a public website. Communication to data subjects is considered helpful in cases, where CSP has by any chance the possibility to support data subjects. As under this Code CSPs are only processors, CSP's possibility are by default very limited. Nonetheless, this should not prevent data subjects to reach out to the Data protection Point of Contact upon request. CSPs may have both, a formal DPO and a Data Protection Point of Ccontact. This control may be met in those cases, if Customers may reach the Data Protection Point of Contact only, provided that such Data Protection Point of Contact can internally escalate any Customer request to the DPO where necessary. Where a CSP has both a DPO and a Data Protection Point of Contact, the notification to supervisory authorities may only entail the contact details of the DPO.							COM-01 Identification of applicable legal, contractual and data protection requirements
[5.10.A] CSP shall establish documented procedures on how to address data subjects' requests.	[5.10.A] CSP should have procedures in place which outline how Customer data subjects' requests are handled by the CSP, taking account of the nature of the processing. **Example**: Policies and procedures should ensure that: ▪ appropriate actions are taken in a timely manner, ▪ data subject identity verification is in place, where appropriate and practicable ▪ CSP either forwards the data subject's request to the Customer(s) concerned or notifies Customer(s) concerned. The CSP may use Customer support mechanisms to notify	Art. 15.1, Art. 28.3 (e)	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.1.1 Obligation to cooperate regarding PII principals' rights	B.8.2.5 Customer obligations B.8.3.1 Obligations to PII principals	CC2.2 CC2.3 P5.1	DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	the Customer, such as: ▪ Customer support mechanism ▪ Customer contact details ▪ DPO contacts ▪ etc.							
[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] CSP should establish procedures which assist the Customer to fully address data subject access requests, taking account of the nature of the processing. **Example**: The CSP may document the methods available to the Customer, outlining options for the Customer in terms of fulfilling data subject requests. The CSP may assist the Customer by: ▪ Identifying data subject access requests received by the CSP from Customer end users ▪ redirecting to the Customer, data subject access requests received by the CSP from Customer end users ▪ assisting the Customer in accessing the personal information of the data subject, taking into account the nature of the processing and the functionality of the service. ▪ providing self-service tools and functionality to assist the Customers end users to access their Customer Personal Data	Art. 28.3 (e)	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.1.1 Obligation to co-operate regarding PII principals' rights	B.8.2.5 Customer obligations B.8.3.1 Obligations to PII principals	P5.1 CC1.1 CC2.2 CC2.3 CC3.1	OIS-03 Authorities and responsibilities in the framework of information security COM-01 Identification of applicable legal, contractual and data protection requirements DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider
[5.11.A] CSP shall establish policies and procedures to enable Customer to respond to requests by supervisory authorities.	[5.11.A] CSP should have policies and procedures 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. **Example**: Procedures should provide that, the CSP in line with other obligations under this Code may make available: ▪ relevant certificate or audit reports, ▪ information about the nature of the Cloud Service, and ▪ additional services etc. This information may be provided under additional confidentiality agreements. The CSP may ensure that: ▪ the Data Protection Point of Contact is available ▪ Customer requests are flagged as requests	Art. 28, Art. 31, Art. 30.4	A.18.1 Compliance with legal and contractual requirements A.6.1.3 Contact with authorities	18.1 Compliance with legal and contractual requirements 6.1.3 Contact with authorities	18.1 Compliance with legal and contractual requirements A.5.1 PII disclosure notification 6.1.3 Contact with authorities A.5.2 Recording of PII disclosures	B.8.5.3 Records of PII disclosure to third parties B.8.5.4 Notification of PII disclosure requests B.8.5.5 Legally binding PII disclosures 6.3.1.3 Contact with authorities	CC1.3 CC1.5 P6.4 P6.7	UP-03 Disclosure and investigatory powers OIS-05 Contact with relevant government agencies and interest groups

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	related to a request by a supervisory authority” and consequently will be processed with high priority - where the information provided by CSP with regards to other obligations under this Code, as making available certificate or audit reports, information about the nature of the Cloud Service, etc, does not fully serve the needs of Customer to respond to the request of a supervisory authority, CSP has established procedures to individually provide the necessary information; this information may be provided under additional confidentiality agreements.							
[5.11.B] CSP shall establish documented procedures to respond to requests by supervisory authorities safeguarding that such responds take place in due time and appropriate detail and quality.	[5.11.B] Policies and procedures should enable the CSP to gather relevant information in due course ensuring that CSP is able to respond to supervisory authorities in appropriate quality and in due time. Such policies and procedures may include aspects like: - Ensuring that the Data Protection Point of Contact is available for supervisory authorities - Supervisory requests are flagged as request by a supervisory authority” and consequently will be processed with high priority - Mechanisms enabling the CSP to promptly provide the fully maintained records of processing activities, if requested							
[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] Conditions for notification of the Customer, if permitted by relevant law, when a CSP receives a request from the supervisory authority relating to Customer Personal Data by the CSP should form part of the Cloud Services Agreement.							
[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.	[5.12.A] CSP should ensure that employees and contractors who are involved in the processing of the Customer Personal Data are subject to appropriate confidentiality obligations. **Example**: As part of CSP’s internal procedures, employees and contractors involved in the processing of the Customer Personal Data should, agree and sign the terms and conditions of their contract relating to confidentiality obligations.	Art. 28.3 (b),	A.18.1 Compliance with legal and contractual requirements A.6.1.1 Information security roles and responsibilities A.7.1.2 Terms and conditions of employment	18.1 Compliance with legal and contractual requirements 6.1.1 Information security roles and responsibilities 7.1.2 Terms and conditions of employment	18.1 Compliance with legal and contractual requirements 7 Human resource security 13.2.4 Confidentiality or non-disclosure agreements	6.4.1.2 Terms and conditions of employment 6.10.2.4Confidentiality or non-disclosure agreements B.8.5.7 Engagement of a subcontractor to process PII	CC2.3 CC3.2 CC1.4 CC2.2 CC6.2 C1.5	SA-01 Documentation, communication and provision of policies and instructions HR-01 Security check of the background information HR-03 Security training and awareness-raising

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
[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.	CSP's policies should, at least, state that employees and contractors who are given access to Customer Personal Data should sign a confidentiality agreement or NDA,or be subject to statutory confidentiality obligations prior to being given access to Customer Personal Data, and outline the actions to be taken if the employee or contractor disregards the confidentiality obligations. The CSP should establish a disciplinary process with respect to employees or contractors who have committed a breach of their confidentiality obligations. Contracts with subprocessors should flow down no less protective measures to the employees and contractors of those subprocessors, who have access to Customer Personal Data. [5.12.B] CSP should 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. Such policies and procedures may entail e.g. ▪ training (for details, please note Control [5.12.E]) ▪ information during onboarding ▪ frequent reminders		A.7.2 During employment A 13.2.4 Confidentiality or non-disclosure agreements	7.2.2 Information security awareness, education and training 13.2.4 Confidentiality or non-disclosure agreements	A.10.1 Confidentiality or non-disclosure agreements	6.12.1 Information security & privacy in supplier relationships		program HR-04 Disciplinary measures HR-05 Termination of the employment relationship or changes to the responsibilities KOS-08 Confidentiality agreement
[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. [5.12.D] Confidentiality obligations contained within the terms and conditions of employment or agreements with contractors or subprocessor shall continue after	[5.12.C] CSP should ensure that Customer Personal Data is only processed by CSP personnel as requested by the Instructions of the Customer, subject to the Cloud Services Agreement. **Example**: Personnel of the CSP should work to defined processes which: ▪ clearly outline Customer Instructions ▪ prevent accidental access to Customer Personal Data ▪ can determine geographical reach of Customer Personal Data processing ▪ contains process sign off for workarounds and/or exceptions to Customer Instructions [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.	Art. 28.3 (b), Art. 32.4	A.18.1 Compliance with legal and contractual requirements A.7 Human resource security A 9.2 User management	18.1 Compliance with legal and contractual requirements 7 Human resource security 9.2 User management	7 Human resource security 13.2.4 Confidentiality or non-disclosure agreements A.10.1 Confidentiality or non-disclosure agreements	B.8.2 Conditions for collection and processing	CC2.2 CC2.3 CC2.1 CC5.2 P4.1	KOS-08 Confidentiality agreement IDM-01 Policy for system and data access authorisations IDM-02 User registration IDM-03 Granting and change (provisioning) of data access authorisations IDM-04 Withdrawal of authorisations (de-provisioning) in case of changes to the employment relationship IDM-05 Regular review of data access authorisations

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
the end of the employment or termination of the agreement.								IDM-06 Administrator authorisations IDM-07 Non- disclosure of authentication information
[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. [5.12.F] Training and awareness shall be subject to timely reviews.	[5.12.E] CSP personnel involved in the processing of the Customer Personal Data should receive periodic training in organizational policies and procedures, as relevant for their role and job function, in conjunction with nature of the Cloud Service. **Example**: The CSP training program should make employees and contractors, role specific, aware of their responsibilities around data protection in line with the CSP's policies and procedures. The awareness and training program may include ▪ web courses, ▪ lectures, ▪ self-study courses, ▪ campaigns (e.g. a data protection, or information security day), ▪ written communications, ▪ newsletters. The program should be planned taking into consideration the roles in the organization. The program should cover security and data protection practices, policies, and procedures. [5.12.F] Training and awareness should be subject to periodic reviews, with regards to its contents, its participation, its quality and effectiveness also with regards to the means training is being provided	Art. 28,	A.7.2.2 Information security awareness, education and training	7.2.2 Information security awareness, education and training	7.2.2 Information security awareness, education and training	6.4.2.2 Information security & privacy awareness, education and training	CC2.2 CC1.4	HR-03 Security training and awareness-raising program
[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] A Cloud Service is understood as capable if the CSP states such capability in the Cloud Service Agreement. *Sufficiently*” in this regard means: to the extent relevant and necessary to provide the Customer with the possibility to take an appropriately informed decision on the engagement of the CSP as a processor. Where applicable, alternate technical and organizational measures for the processing of Special Categories of Personal Data may be implemented depending on the nature	Art. 9.3, Art. 32	A.18.1 Compliance with legal and contractual requirements A.8.2 Information classification	18.1 Compliance with legal and contractual requirements 8.2 Information classification	18.1 Compliance with legal and contractual requirements	B.8.2 Conditions for collection and processing 6.5.1.3 Acceptable use of assets 6.5.2.1 Classification of information	CC3.1 CC4.1	COM-01 Identification of applicable legal, contractual and data protection requirements

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	of the Special Category of Personal Data that is being processed. **Examples of appropriate technical & organisational measures** To the extent a Cloud Service is capable of processing health data, the CSP may consider alternative ap-propriate technical and organizational measures as: ■ encryption mechanisms; ■ limitation of data access; ■ and any additional technical and organizational measures as required by regulatory/compliance frameworks If Customer requests information from CSP related to compliance with national Member State law, sufficient communication will include appropriate responses in this regard as well.							
[5.13.A] CSP shall establish procedures to ensure the reporting of data breaches to the Customer through appropriate channels without undue delay. [5.13.B] CSP shall specify its data breach notification obligations as well as its	[5.13.A] CSP should have incident management procedures in place which ensure that data breaches can be reported to the Customer through appropriate channels without undue delay. **Example**: ISO 27002 16.1.1. should serve as non-compulsory guidelines. If a data breach has been detected, the CSP should ensure that the Customer is informed without undue delay. Elements of Breach reporting procedures may include: ■ Roles and Responsibilities - of the Incident management team ■ Investigation - determining the fact and evaluating the risk and who may be affected ■ Communication - determining a notification process depending on the circumstances and nature of the Incident ■ Recordkeeping: keeping a record of what was done and by whom to help in later analysis ■ Audit: conducting root cause analysis and remediation planning Breach Management by the CSP, should be in accordance with Article 29 and EDPB guidance: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 [5.13.B] As part of the Cloud Services Agreement, the CSP shall specify its data breach notification obligations as	Art. 33	A.18.1 Compliance with legal and contractual requirements A.16.1 Management of information security incidents and improvements	18.1 Compliance with legal and contractual requirements 16.1 Management of information security incidents and improvements	18.1 Compliance with legal and contractual requirements 16.1 Management of information security incidents and improvements A.9.1 Notification of a data breach involving PII	6.13.1 Management of information security incidents and improvements	CC3.3 CC6.1 CC2.3 P6.3 P6.5 P6.2	SIM-01 Responsibilities and procedural model SIM-02 Classification of Customer systems SIM-03 Processing of security incidents SIM-04 Documentation and reporting of security incidents SIM-05 Security incident event management SIM-06 Duty of the users to report security incident to a central body

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
technical and organizational measures to detect, mitigate and report a data breach in the Cloud Service Agreement.	well as its technical and organizational measures to detect, mitigate and report a data breach in the Cloud Service Agreement. ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management” may serve a non-compulsary guideline.							
[5.14.A] CSP shall provide a capability for the Customer to retrieve the Customer Personal Data promptly and 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.A] Whereas the technical means may be of different, but same effective manner, those means should ideally be accessible to Customers at any time, but certainly on termination of the Cloud Service. *Means*” may include e.g. ▪ where a Customer Portal with self-service is available for the Customer to retrieve or delete Customer Personal Data, the CSP should communicate to the Customer of its availability in the Cloud Services Agreement; ▪ where the CSP may not have access or control of the data, Customer’s responsibility to retrieve and delete the data should be communicated to the Customer. For the avoidance of doubt: To the extent Customer entrusted Customer Personal Data by handing over dedicated hardware, such as hard drives, retrieval should be handing back such hard drives. To the extent Customer entrusted Customer Personal Data by copying such data into the Cloud Service retrieval is expected to be the provisions of a complete copy of such data, as this is a technical necessity. In cases where Customer entrusted hardware and Cloud Service resulted into additional Customer Personal Data, that are not necessarily processed on such dedicated Customer hardware, retrieval should cover both: handing back Custer hardware plus retrieval of a complete copy of any additional Customer Personal Data. [5.14.B] The offboarding process of a Customer may be different taking into account the nature of the processing, agreed upon needs of Customers as well as amount and complexity of Customer Personal Data being processed. **Examples** The termination of a Cloud Service may result into a prompt automated and full deletion or return and deletion upon any notification period expiry. In those cases, as agreed upon, Customer is responsible for timely exporting its Customer Personal Data. The CSP should indicate	Art. 28.3 (g)	A.18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements	18.1 Compliance with legal and contractual requirements A.9.3 PII return, transfer and disposal	B.8.4.2 Return, transfer or disposal of PII	CC1.2 P2.1	PI-01 Use of public APIs and industry standards PI-02 Export of data PI-03 Policy for the portability and interoperability PI-04 Secure data import and export

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	Customer's responsibility when it terminates the Cloud Service. Alternatively, and as agreed upon in the Cloud Service Agreement, the termination of a Cloud Services may initiate a tiered approach and thus suspend the deletion or return and deletion. Such a tiered approach may include: ■ offering Customer possibilities to configure and thus limit processing capabilities and access due to Customer User roles, such as by offering Customers to turn on a maintenance mode", that will e.g. limit any access to Customer Personal Data by Customer users besides Customer admins; ■ Offering an additional period for the sole purposes of expoting and/or deletion of Customer Personal Data as agreed upon in the Cloud Service Agreement; ■ transferring Customer Personal Data into a e.g. dedicated, encrypted and access-limited storage to enable Customer convenient re-onboarding within a designated period of time, as agreed upon in the Cloud Service Agreement. CSP may charge fees, as agreed upon in the Cloud Service Agreement, for whatever services the CSP keeps providing after the notification period for the commercial Cloud Service has passed. Where the CSP opts for a tiered approach, deletion or return and deletion of Customer Personal Data needs to be ensured for moment any designated period passes.							
[5.14.C] CSP shall provide the Customer Personal Data in a machine readable, commonly used, structured format.	[5.14.C] The provided Customer Personal Data needs to be in a machine-readable, commonly used and structured format and this format should be fully described in documentation available to the Customer on request. **Example** In this context "*Commonly Used*" refers to Cloud industry standard formats, as determined by the nature of the given Cloud Service.							
[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] Where requested the CSP shall provide the Customer with a description of the format and mechanisms to provide the Customer Personal Data. Please note Control Guidance of Control [5.14.A] in this							

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016
	regard. Addtionally, this may include a description of the structure of the formats being offered. In this regard, please also note Control Guidance of Control [5.14.C].							
[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.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.E] CSP should ensure the Cloud Services Agreement specifies deletion and return timelines of Customer Personal Data. The CSP may retain certain data where required by law or regulations. [5.14.F] CSP should maintain an appropriate media disposal and/or data wiping procedure to govern storage media no longer in use. **Example**: Appropriate media disposal policies may include: ■ Instructions for physically destroying the media so that it can no longer be used ■ Secure deletion software - This involves using software to overwrite data . ■ Use of specialist third parties - There are many organisations which will securely delete data from a range of devices and types of media. These organisations will destroy or overwrite your data on your behalf. ■ Formatting media - to recreate the data structures and file system NIST guidance for Media Sanitization can be viewed as non-compulsory guidance: ■ **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). ■ **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques. ■ **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data. https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final	Art. 28.3 (g), Art. 32.2	A.18.1 Compliance with legal and contractual requirements A.8.3 Media handling	18.1 Compliance with legal and contractual requirements 8.3 Media handling	18.1 Compliance with legal and contractual requirements A.9.3 PII return, transfer and disposal A.10.7 Secure disposal of hardcopy materials A.10.13 Access to data on pre-used data storage space A.4.1 Secure erasure of temporary files	B.8.2.1 Customer agreement B.8.4.1 Temporary files B.8.4.2 Return, transfer or disposal of PII 6.5.3 Media handling	CC6.5 C1.2 CC3.1 P4.3	PI-05 Secure deletion of data AM-04 Handing in and returning assets COM-01 Identification of applicable legal, contractual and data protection requirements

3 Controls of Section 6, Control Guidance and Mapping with International Standards

Controls of Section 6 have been mapped against controls of internationally recognized standards, including ISO/IEC 27001:2013, ISO/IEC 27018:2019, ISO/IEC 27701:2019, SOC 2, Cloud Computing Compliance Controls Catalog ("C5"), as well as NIST SP 800-53 Rev5[1] and NIST Cybersecurity Framework v1.1 ("Cybersecurity Framework")[2], that are considered to be equal but not less protective than the Controls of the Code.

Please note: GDPR mapping is considered a starting point which GDPR provisions relate to the Control; GDPR mapping is not intended to provide an exhaustive and binding reference of which GDPR provision is being thoroughly particualrized. Consequently, compliance with the respective Controls does not necessarily relate to an exhaustive compliance with the provided GDPR provisions.

[1] Accessible at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[2] Accessible at https://www.nist.gov/cyberframework/framework.

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cyberecurity Framework
[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.A] CSP should implement appropriate organizational 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. [6.1.B] To address the sensitivity of Customer Personal Data accordingly the CSP may – depending on the nature of processing – e.g. ▪ classify Customer Personal Data, establish appropriate measures for each type of classified Customer Personal Data; ▪ determine the type of Customer Personal Data being processed by the Cloud Service that requires the highest level of protection and apply respective measures to all Customer Personal Data that is being processed. Where the CSP provides Cloud Services with dedicated functionalities related to specific data, the CSP may refer to such functionalities to determine the type of Customer Personal Date being processed. CSP may additionally specifiy types of Customer Personal Data that is permited or prohibited to being processed in the Cloud Service or using specific features or functionalities thereof. There may be also occasions where CSP may and must not know the type of Customer Personal Data. In those cases the CSP may transparently communicate its technical and organizational measures to Customers. Please note the Controls [5.12.G and 5.12.H].	Art. 28.3 (c), Art. 28.3 (f)	A.8.2 Information classification A.5 Information security policies	A.8.2.2 Labelling of information	5.1.1 Policies for information security 8.2 Information classification	B.8.4 Privacy by design and privacy by default	C1.1 A1.1	SIM-02 Classification of Customer systems AM-05 Classification of information AM-06 Labelling of information and handling of assets	Access publicly available PDF version: NIST SP 800-53 AC-16 – Security and Privacy Attributes PE-19 – Information Leakage PM-5 – System Inventory PT-1 – Policies and Procedures PT-2 – Authority to Process PII PT-7 – Specific Categories of PII RA-8 – Privacy Impact Assessments SA-3 System Development Life Cycle SA-8 – Security and Privacy Engineering Principles SC-28 – Protection of Information at Rest	ID.AM: Asset Management ID.AM-1 ID-AM-2 ID-AM-3 ID.AM-4 PR.AC: Identity Management. Authentication, and Access Control PR.AC-1 PR.AC-2 PR.AC-3 PR.AC-4 PR.AC-5 PR.AC-6 PR.AC-7
[6.1.C] The CSP shall establish, implement, maintain and continually improve an information security management system (ISMS), in accordance with the requirements of	[6.1.C] CSP should document information determined by the CSP as being necessary for the effectiveness of the ISMS. An ISMS is the organizational structure, guidelines, procedures, policies and resources that					6.1 General	CC3.1 CC3.2 CC4.1	OIS-01 Information security management system (ISMS)	Access publicly available PDF version: NIST SP 800-53 PM-1 – Information Security Program Plan	ID.GV: Governance ID.GV-1 ID.GV-2 ID.GV-3

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cyberecurity Framework
ISO 27001 or any equivalent International Standards.	enables an organisation to, establish, implement, operate, monitor, maintain and improve information security within the organization based on a business risk approach. Key elements of an ISMS include: 1. **Context of the organization** ■ Understanding the organization and its context ■ Understanding the needs and expectations of interested parties ■ Determining the scope of the information security management system ■ Information security management system 2. **Leadership** ■ Leadership and commitment ■ Policy ■ Organizational roles, responsibilities and authorities 3. **Planning** ■ Actions to address risks and opportunities ■ Information security objectives and planning to achieve them 4. **Support** ■ Resources ■ Competence ■ Awareness ■ Communication ■ Documented information 5. **Operation** ■ Operational planning and control ■ Information security risk assessment ■ Information security risk treatment 6. **Performance evaluation** ■ Monitoring, measurement, analysis and evaluation ■ Internal audit ■ Management review 7. **Improvement** ■ Nonconformity and corrective action ■ Continual improvement								PM-2 – Information Security Program Leadership Role PM-3 - Information Security and Privacy Resources PM-4 – Plan of Action and Milestone Process PM-5 – System Inventory PM-6 – Measures of Performance PM-7 – Enterprise Architecture PM-8 – Critical Infrastructure Plan PM-9 – Risk Management Strategy PM-10 – Authorization Process PM-11 – Mission and Business Process Definition PM-12 – Insider Threat Program PM-13 – Security and Privacy Workforce PM-14 – Testing, Training, and Monitoring PM-15 – Security and Privacy Groups and Associations PM-16 – Threat Awareness Program PM-17 – Protecting Controlled Unclassified Information on External Systems PM-18 Privacy Program Plan	ID.GV-4 ID.RM: Risk Management Strategy ID.RM-1 ID.RM-2 ID.RM-3
[6.1.D] The CSP shall establish a process to determine the	[6.1.D] CSP should analyse the Code and this Controls Catalogue thorouhgly. Where									

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cyberecurity Framework
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.	specific Controls of this Section fall outside the ISMS, there may be different ways of documentation, especially where a CSP provides several Cloud Services: - where multiple Cloud Services share the reasons why Controls do not apply, this may be documented once provided that this documentation can be easily provided to the Monitoring Body and Supervisory Authority, e.g. y being referened to the Cloud Services concerned; - where specific Controls do not apply due to the nature of processing (including the type of Cloud Service, e.g. IaaS, SaaS, PaaS) this may be documented once, provided that this documentation can be easily provided to the Monitoring Body and Supervisory Authority, e.g. by being referenced to the Cloud Services concerned; Regarding alternative measures, the reasoning and evidence may be provided during the process of declaring a Cloud Service adherent. Documentation should be prepared at least in a way that all relevant information can be easily gathered upon request, e.g. by internal (file) references.								PM-28 – Risk Framing PM-29 – Risk Management Program Leadership Roles PM-30 – Supply Chain Risk Management Strategy	
Objective 1 - Management direction for information security [6.2.A] The controls set out in ISO 27001 control domain A5 or equivalent International Standard, but no less protective, shall be implemented.	[6.2.A] The implementation guidance provisions of ISO 27002 control domain A 5. are to be understood as non-compulsory guidelines. This includes clear management-level direction and support for the security of Customer Personal Data processed by the CSP's Cloud Services, as well as management-approved set of information security policies that govern the security of Cloud Services Customer Personal Data in the CSP's Cloud Services.		A.5 Information security policies	5.1.1 Policies for information security A.18.2.1 Independent review of information security	5.1.1 Policies for information security 5.1.2 Review of the policies for information security	6.2 Information Security & Privacy Policies	CC2.3 CC3.2 CC4.1	SA-01 Documentation, communication and provision of policies and instructions COM-02 Planning independent, external audits COM-03 Carrying out independent, external audits	Access publicly available PDF version: NIST SP 800-53 3.13 PROGRAM MANAGEMENT PM-1 – Information Security Program Plan PM-2 – Information Security Program Leadership Role 3.1 ACCESS CONTROL AC-1 – Policies and Procedures	ID.GV: Governance ID.GV-1 – Organizational cybersecurity policy

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cybercurity Framework
									3.2 AWARENESS AND TRAINING AT-1 - Policies and Procedures 3.3 AUDIT AND ACCOUNTABILITY AU-1 – Policies and Procedures 3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING CA-1 – Policies and Procedures 3.5 CONFIGURATION MANAGEMENT CM-1 - Policies and Procedures 3.6 CONTINGENCY PLANNING CP-1 - Policies and Procedures 3.7 IDENTIFICATION AND AUTHENTICATION IA-1 - Policies and Procedures 3.8 INCIDENT RESPONSE IR-1 - Policies and Procedures 3.9 MAINTENANCE MA-1 - Policies and Procedures 3.10 MEDIA PROTECTION MP-1 - Policies and Procedures 3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION PE-1 - Policies and Procedures 3.12 PLANNING PL-1 - Policies and Procedures	

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cyberecurity Framework
									3.14 PERSONNEL SECURITY PS-1 - Policies and Procedures 3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY PT-1 - Policies and Procedures 3.16 RISK ASSESSMENT RA-1 - Policies and Procedures 3.17 SYSTEM AND SERVICES ACQUISITION SA-1 - Policies and Procedures 3.18 SYSTEM AND COMMUNICATIONS PROTECTION SC-1 - Policies and Procedures 3.19 SYSTEM AND INFORMATION INTEGRITY SI-1 - Policies and Procedures 3.20 SUPPLY CHAIN RISK MANAGEMENT SR-1 - Policies and Procedures	
Objective 2 - Organisation of information security [6.2.B] The controls set out in ISO 27001 control domain A6 or equivalent International Standard, but no less protective, shall be implemented.	[6.2.B] The implementation guidance provisions of ISO 27002 control domain A 6. are to be understood as non-compulsory guidelines. This includes a management structure to manage the implementation of information security within the CSP's Cloud Services, with clear roles and responsibilities within the organisation.		A.6 Organization of information security	A.6.1.1 Information security roles and responsibilities	6.1.1 Information security roles and responsibilities	6.3 Organization of information security	CC1.1 CC3.1 CC3.2 CC4.1 CC2.2 CC2.3	OIS-01 Information security management system (ISMS) OIS-02 Strategic targets regarding information security and responsibility of the top management	Access publicly available PDF version: NIST SP 800-53 PM-3 – Information Security and Privacy Resources PM-15 – Security And Privacy Groups And Associations AC-5 – Separation Of Duties AC-6 – Least Privilege	ID.GV: Governance ID.GV-2: Cybersecurity Roles and Responsibilities

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cybercurity Framework
									SI-5 – Security Alerts, Advisories, And Directives	
Objective 3 Human resources security [6.2.C] The controls set out in ISO 27001 control domain A7.1 and A7.2 or equivalent International Standard, but no less protective, shall be implemented.	[6.2.C] The implementation guidance provisions of ISO 27002 control domain A.7.1 and A.7.2 are to be understood as non-compulsory guidelines. Additional guidance can be sought from ISO 27018 A.10.1. This includes all appropriate steps to ensure that all employees, contractors and other individuals, within the CSP's control, who have access to Customer Personal Data, are aware of and understand their information security responsibilities and have suitable qualifications and capabilities for their roles within the CSP and to have an appropriate mechanisms in place to monitor and support compliance with these policies and related obligations.		A.7.1 Prior to employment A.7.2 During employment	A.7.2.2 Information security awareness, education and training	7.1 Prior to employment 7.2 During employment A.10.1 Confidentiality or non-disclosure agreements	6.4 Human resource security	CC1.4 CC2.2 CC1.5	HR-01 Security check of the background information HR-03 Security training and awareness-raising program HR-04 Disciplinary measures HR-05 Termination of the employment relationship or changes to the responsibilities	Access publicly available PDF version: NIST SP 800-53 PS-1 – Policies and Procedures PS-2 – Position Risk Description PS-3 – Personnel Screening PS-4 – Personnel Termination PS-5 – Personnel Transfer PS-6 – Access Agreements PS-7 – External Personnel Security PS-8 – Personnel Sanctions PS-9 – Position Descriptions	PR.AT: Awareness and Training PR.AT-1 – All users PR.AT-2 – Privileged Users PR.AT-3 – Third-party Stakeholders PR.AT-4 – Senior Executives PR.AT-5 – Physical and cybersecurity personnel PR.IP: Information Protection Processes and Procedures PR.IP-11 – Cybersecurity in HR practices
Objective 4 - Asset management [6.2.D] The controls set out in ISO 27001 control domain A8 or equivalent International Standard, but no less protective, shall be implemented. [6.2.E] The controls set out in ISO 27001 control domain A11.2 or equivalent International Standard, but no less protective, shall be implemented.	[6.2.D] The implementation guidance provisions of ISO 27002 control domain A.8 are to be understood as non-compulsory guidelines. [6.2.E] The implementation guidance provisions of ISO 27002 control domain A.11.2 are to be understood as non-compulsory guidelines. Additional guidance can be sought from ISO 27018 A.10.4 and A.10.13. This includes all appropriate steps to ensure the security and confidentiality of the CSP's		A.8 Asset management A.11.2 Equipment	A.8.1.1 Inventory of assets A.8.1.2 Ownership of assets A.8.2.3 Handling of assets	8 Asset management	6.5 Asset management	CC2.2 CC2.3 C1.1 A1.1 CC6.1 CC6.4 CC6.5 CC6.7	AM-01 Asset inventory AM-02 Assignment of persons responsible for assets AM-03 Instruction manuals for assets AM-04 Handing in and returning assets AM-05 Classification of information AM-06 Labelling of information and handling of assets	Access publicly available PDF version: NIST SP 800-53 CM-8 – System Component Inventory PE-1 – Policy And Procedures PE-20 – Asset Monitoring and Tracking PM-5 – System Inventory RA-2 – Security Categorization MP-1 – Policy And Procedures	ID.AM: Asset Management AD.AM-1 – Physical Devices and Systems

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cybercurity Framework
	assets and facilities associated with the processing of Customers' data, with policies for deleting or rendering Customer Personal Data unrecoverable.							AM-07 Management of data media AM-08 Transfer and removal of assets		
Objective 5 - Access controls [6.2.F] The controls set out in ISO 27001 control domain A9 or equivalent International Standard, but no less protective, shall be implemented.	[6.2.F] The implementation guidance provisions of ISO 27002 control domain A.9 are to be understood as non-compulsory guidelines. Additional guidance can be sought from ISO 27018 A.9.2. This includes to limit access to Customer Personal Data, both in the cloud and the facilities in which the Customer Personal Data is processed, including through logical access controls.		A.9 Access control	A.9.2.1 User registration and de-registration A.9.2.2 User access provisioning A.9.4.1 Information access restriction	9.1 Business requirements of access control 9.2 User access management 9.3 User responsibilities 9.4 System and application access control	6.6 Access control	CC6.1 CC6.4 CC6.2	IDM-01 Policy for system and data access authorisations IDM-02 User registration IDM-03 Granting and change (provisioning) of data access authorisations IDM-04 Withdrawal of authorisations (de-provisioning) in case of changes to the employment relationship IDM-05 Regular review of data access authorisations IDM-06 Administrator authorisations IDM-07 Non- disclosure of authentication information	Access publicly available PDF version: NIST SP 800-53 AC-1 – Policy and Procedures AC-2 – Account Management AC-3 – Access Enforcement AC-4 – Information Flow Management AC-5 – Separation of Duties AC-6 – Least Privilege AC-7 – Unsuccessful Logon Attempts AC-8 – System Use Notification AC-9 - Previous Logon Information AC-10 – Concurrent Session Control AC-11 – Device Lock AC-12 – Session Termination AC-14 – Permitted Actions without Identification or Authentication AC-16 – Security and Privacy Attributes AC-17 – Remote Access AC-18 – Wireless Access AC-19 – Access Control for Mobile Devices	PR.AC: Identity Management, Authentication and Access Control PR.AC-1 – Devices, users, and processes PR.AC-2 – Physical access to assets PR-AC-3 – Remote access PR.AC-4 – Access permissions PR.AC-5 – Network integrity PR.AC-6 – Identity proofing PR.AC-7 - Authentication

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cybercurity Framework
									AC-20 – Use of External Systems AC-21 – Information Sharing AC-22 – Publicly Accessible Content AC-23 – Data Mining Protection AC-24 – Access Control Decisions AC-25 – Reference Monitor	
Objective 6 - Encryption [6.2.G] The controls set out in ISO 27001 control domain A10 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. [6.2.I] To the extent CSP provides encryp-tion capabilities such capabilities shall be implemented effectively, i.e. by following strong and trusted techniques, taking into account the state-of-the-art,	[6.2.G] The implementation guidance provisions of ISO 27002 control domain A.10 and A.13.2 are to be understood as non-compulsory guidelines. Additional guidance can be sought from ISO 27018 A.10.1.1. [6.2.H] CSP should have appropriate procedures to support Customer by implementing encryption in line with industry best practices and relevant regulations. This includes, where technically feasible and operationally practicable (including based on the nature of the Cloud Service), to make available and/or implement encryption controls at least for any transit of data to protect the confidentiality of Customer Personal Data in the cloud, where provided for in the Cloud Services Agreement or where considered necessary based on a risk analysis. [6.2.I] Implementing adequate encryption is complex. To keep the Code flexible and future-proof the Code does not provide distinct algorithm or techniques. However, to the extent CSP implemented encryption capabilities, CSP needs to be able to reason its actual implementation, especially why the		A.10 Cryptography A.13.2 Information transfer	A.10.1.1 Policy on the use of cryptographic controls	10.1.1 Policy on the use of cryptographic controls 10.1.2 Key management A.10.4 Protecting data on storage media leaving the premises A.10.6 Encryption of PII transmitted over public data-transmission networks	6.7 Cryptography	CC6.1 CC6.7	KRY-01 Policy for the use of encryption procedures and key management KRY-02 Encryption of data for transmission (transport encryption) KRY-03 Encryption of sensitive data for storage KRY-04 Secure key management	Access publicly available PDF version: NIST SP 800-53 SC-8 – Transmission Confidentiality and Integrity SC-12 – Cryptographic Key Establishment and Management SC-13 – Cryptographic Protection SC-16 – Transmission of Security and Privacy Attributes SC-17 – Public Key Infrastructure Certificates	PR.DS-1: Data-at-rest protection PR.DS-2: Data-in-transit protection

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cyberecurity Framework
adequately preventing abusive access to Customer Personal Data.	implementation adequately prevents from abusive access. Adequacy should take into account the assessment as performed under [6.1.A] and [6.1.B].									
Objective 7 - Physical and environmental security [6.2.J] The controls set out in ISO 27001 control domain A11, or equivalent International Standard, but no less protective, shall be implemented.	[6.2.J] The implementation guidance provisions of ISO 27002 control domain A.11 are to be understood as non-compulsory guidelines. This includes physical and environmental security measures, designed to prevent unauthorized access, alteration to or destruction of Customer Personal Data in the cloud and to the related information processing facilities.		A.11 Physical and environmental security	A.11.2.7 Secure disposal or reuse of equipment	11.1.1 Physical security perimeter 11.1.2 Physical entry controls 11.1.3 Securing offices, rooms and facilities 11.1.4 Protecting against external and environmental threats 11.2 Equipment A.10.13 Access to data on pre-used data storage space	6.8 Physical and environmental security	CC6.5 CC6.4 A1.2	PS-01 Perimeter protection PS-02 Physical site access control PS-03 Protection against threats from outside and from the environment PS-04 Protection against interruptions caused by power failures and other such risks PS-05 Maintenance of infrastructure and devices	Access publicly available PDF version: NIST SP 800-53 PE-1 – Policy and Procedures PE-2 – Physical Access Authorizations PE-3 – Physical Access Control PE-4 – Access Control for Transmission PE-5 – Access Control for Output Devices PE-6 – Monitoring Physical Access PE-8 – Visitor Access Records PE-9 – Power Equipment and Cabling PE-10 – Emergency Shutoff PE-11 – Emergency Power PE-12 – Emergency Lighting PE-13 – Fire Protection PE-14 – Environmental Controls PE-15 – Water Damage Protection PE-16 – Delivery and Removal PE-17 – Alternate Work Site PE-18 – Location of	PR.AC-2 – Physical access to assets PR.IP-5 – Physical operating environment for assets DE.CM-2: Physical environment monitoring

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cyberecurity Framework
									System Components PE-19 – Information Leakage PE-20 – Asset Monitoring and Tracking PE-21 – Electromagnetic Pulse Protection PE-22 – Component Marking PE-23 – Facility Location	
Objective 8 – Operational security [6.2.K] The controls set out in ISO 27001 control domain A12, or equivalent International Standard, but no less protective, shall be implemented.	[6.2.K] The implementation guidance provisions of ISO 27002 control domain A.12 are to be understood as non-compulsory guidelines. This includes, to the extent the CSP is responsible for the Customer Personal Data in the operations of the Cloud Service, all appropriate steps to ensure the secure operation of facilities and services that are involved in the CSP's processing of a Customer Personal Data; among the procedures to be highlighted: redundancy or internal back-ups of Customer Personal Data and controls on changes to the CSP's data processing facilities and systems that affect Customer Personal Data security.		A.12 Operations security	12 Operations security	12 Operations security	6.9 Operations security	CC2.2 CC2.3 A1.1 A1.2 A1.3 CC6.1 CC6.2 CC4.1 CC7.1	RB-01, 02, 03, 04 Capacity management – planning, monitoring, data location, control of resources RB-05 Protection against malware RB-06,07,08,09 Data backup and restoration – concept, monitoring, regular tests, storage RB-10,11,12,13,14,15,16 Logging and monitoring – concept, meta data, critical assets, storage of the logs, accountability, configuration, availability of the monitoring software RB-17,18,19,20,21,22 Handling of vulnerabilities, malfunctions and errors – concept, penetration tests, integration with change and incident management, involvement of the cloud Customer, check of	Access publicly available PDF version: NIST SP 800-53 SC-38 – Operations Security SR-7 – Supply Chain Operations Security AC-5 – Separation of Duties CM-9 – Configuration Management Plan CP-9 – System Backup Audit and Accountability Family AU-1 – Policy and Procedures AU-2 – Event Logging AU-3 – Content of Audit Records AU-4 – Audit Log Storage Capacity AU-5 – Response to Audit Logging Process Failures AU-6 – Audit Record Review, Analysis, and Reporting AU-7 – Audit Record Reduction and Report	ID.RA-1 – Asset vulnerabilities ID.RA-2 – Cyber threat intelligence ID.RA-3 – Threat documentation ID.RA-5 – Risk determination PR.IP-4 – Backups PR.IP-12 – Vulnerability management plan

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cyberecurity Framework
								open vulnerabilities, system hardening RB-23 Segregation of stored and processed data of the cloud Customers in jointly used resources	Generation AU-8 – Time Stamps AU-9 – Protection of Audit Information AU-10 – Non-Repudiation AU-11 – Audit Record Retention AU-12 – Audit Record Generation AU-13 – Monitoring for Information Disclosure AU-14 – Session Audit AU-16 – Cross-Organizational Audit Logging SC-49 – Hardware-Enforced Separation and Policy Enforcement SC-50 – Software-Enforced Separation and Policy Enforcement CM-11 – User-Installed Software RA-8 – Vulnerability Monitoring and Scanning	
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.	[6.2.L] The implementation guidance provisions of ISO 27002 control domain A13 are to be understood as non-compulsory guidelines. Additional guidance can be sought from ISO 27018 A.13.2.1. This includes all appropriate steps designed to ensure the protection of Cloud Services Customer Personal Data in the CSP's networks and in the CSP's information processing facilities and to ensure the secure transfer of such data or to implement other appropriate security measures feasible in		A.13 Communications security	A.13.1.3 Segregation in networks	13 Communications security	6.10 Communications security	CC6.6 CC6.7	KOS-01 Technical safeguards KOS-02 Monitoring of connections KOS-03 Cross-network access KOS-04 Networks for administration KOS-05 Segregation of data traffic in jointly used network environments	Access publicly available PDF version: NIST SP 800-53 AC-4 – Information Flow Enforcement AC-10 – Concurent Session Control SC-7 – Boundary Protection SC-8 – Transmission Confidentiality And Integrity	PR.AC-5 - Protection of Network Integrity

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cybercurity Framework
	transferring such data in the CSP's networks and processing facilities.							KOS-06 Documentation of the network topology KOS-07 Policies for data transmission KOS-08 Confidentiality agreement		
Objective 10 - System development and maintenance [6.2.M] The controls set out in ISO 27001 control domain A14, or equivalent International Standard, but no less protective, shall be implemented.	[6.2.M] The implementation guidance provisions of ISO 27002 control domain A.14 are to be understood as non-compulsory guidelines. This includes all appropriate steps to ensure that information security is a central part of any new developments to the relevant Cloud Service assets that it uses to process Customer Personal Data.		A.14 System acquisition, development and maintenance	A.14.1.1 Information security requirements analysis and specification A.14.2.1 Secure development policy A.14.2.9 System acceptance testing	14 System acquisition, development and maintenance	6.11 System acquisition, development and maintenance	CC8.1	BEI-01 Policies for the development/procurement of information systems BEI-02 Outsourcing of the development BEI-03 Policies for changes to information systems BEI-04 Risk assessment of changes BEI-05 Categorisation of changes BEI-06 Prioritisation of changes BEI-07 Testing changes BEI-08 Rollback of changes BEI-09 Review of proper testing and approval BEI-10 Emergency changes BEI-11 System landscape BEI-12 Separation of	Access publicly available PDF version: NIST SP 800-53 SA-1 – Policy and Procedures SA-2 – Allocation of Resources SA-3 – System Development Life Cycle SA-4 – Acquisition Process SA-5 – System Documentation SA-8 – Security and Privacy Engineering Principles SA-9 – External System Services SA-10 = Developer Configuration Management SA-11 – Developer Testing and Evaluation SA-15 – Development Process, Standards, and Tools SA-16 – Developer Provided Training SA-17 – Developer Security and Privacy Architecture and Design SA-20 – Customized	PR.IP: Information Protection Processs and Procedures PR.IP-1 PR.IP-2 PR.IP-3

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cyberecurity Framework
								functions	Development of Critical Components SA-21 – Developer Screening SA-22 – Unsupported System Components SA-23 – Specialization	
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.	[6.2.N] The implementation guidance provisions of ISO 27002 point A.15 are to be understood as non-compulsory guidelines. This includes all appropriate steps to ensure that Customer Personal Data is adequately protected where the CSP's subprocessors have access to the CSP's cloud systems or assets.		A.15 Supplier relationships	A.15.1.2 Addressing security within supplier agreements A.15.1.3 Information and communication technology supply chain	15 Supplier relationships A.10.12 Subcontracted PII processing:	6.12 Supplier relationships	CC9.2 CC6.4 CC6.5	DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider	Access publicly available PDF version: NIST SP 800-53 SR-1 – Policy and Produres SR-2 – Supply Chain Risk Management Plan SR-3 – Supply Chain Controls and Processes SR-4 – Provenance SR-5 – Acquisition Strategies, Tools, and Methods SR-6 – Supplier Assessments and Reviews SR-7 – Supply Chain Operations Security SR-8 – Notification Agreements SR-9 – Tamper Resistance and Detection SR-10 – Inspection of Systems or Components SR-11 – Component Authenticity SR-12 – Component Disposal	ID.SC: Supply Chain Risk Management ID.SC-1 ID.SC-2 ID.SC-3 ID.SC-4 ID.SC-5
Objective 12 - Information security incident management [6.2.O] The controls set out in ISO 27001 control domain A16, or equivalent	[6.2.O] The implementation guidance provisions of ISO 27002 control domain A.16 are to be understood as non-compulsory guidelines.		A.16 Information security incident management	A.16.1.1 Responsibilities and procedures A.16.1.2 Reporting information	16 Information security incident management A.9.1 Notification of a data breach	6.13 Information security incident management	CC7.3 CC7.2 CC7.4 CC7.5	SIM-01 Responsibilities and procedural model SIM-02 Classification of Customer systems SIM-03 Processing of	Access publicly available PDF version: NIST SP 800-53 IR-1 – Policy and	PR.IP-9 – Response and Recovery Plans in Place PR.IP-10 – Response and Recovery Plans Tested

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cybercecurity Framework
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.	[6.2.P] CSP should formally adopt and communicate an information security incident management plan to identify, document, and remediate incidents which could impact the availability, confidentiality, security or data protection of the Customers' data as well as the Data Breach response procedures. Information security incident management plan should include communication mechanisms to notify Customers or competent authorities in relation to Customer Personal Data breaches, see Control 5.12.A and 5.12.B of this Code. This includes the development, implementation and management of policies and procedures enabling an effective response to and (where legally required) communication to the Customer, data subjects or competent authorities in relation to personal data breaches.			security events A.16.1.7 Collection of evidence	involving PII			security incidents SIM-04 Documentation and reporting of security incidents SIM-05 Security incident event management SIM-06 Duty of the users to report security incident to a central body SIM-07 Evaluation and learning process	Procedures IR-2 – Incident Response Training IR-3 – Incident Response Testing IR-4 – Incident Handling IR-5 – Incident Monitoring IR-6 – Incident Reporting IR-7 – Incident Response Assistance IR-8 – Incident Response Plan IR-9 – Information Spillage Response	RS.CO-2 – Incident Reporting RS.AN-2 – Incident Impact RS.AN-4 – Inident Categorization RS.MI-1 – Incident Containment RS,MI-2 – Incident Mitigation
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.	[6.2.Q] The implementation guidance provisions of ISO 27002 control domain A.17 are to be understood as non-compulsory guidelines This includes, to the extent the CSP is responsible for the Customer Personal Data in the operations of the Cloud Service, all appropriate steps to ensure that information security continuity, with respect to Customer Personal Data, in the Cloud Service is integrated into the CSP's business continuity management policies, procedures and systems to ensure appropriate security and availability of Customer Personal Data in adverse situations, e.g., a disaster.		A.17 Information security aspects of business continuity management	N/A	17 Information security aspects of business continuity management	6.14 Information security aspects of business continuity management	CC7.5 A1.2 A1.3	BCM-01 Top management responsibility BCM-02 Business impact analysis policies and procedures BCM-03 Planning business continuity BCM-04 Verification, updating and testing of the business continuity BCM-05 Supply of the computing centres	Access publicly available PDF version: NIST SP 800-53 CP-1 – Policy and Procedures CP-2 – Contingency Plan CP-3 – Contingency Training CP-4 – Contingency Plan Testing CP-6 – Alternate Storage Site CP-7 – Alternate Processing Site CP-8 – Telecommunications Services CP-9 – System Backup	PR.IP-9 – Response and Recovery Plans in Place

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cybercurity Framework
									CP-10 – System Recovery and Reconstitution CP-11 – Alternate Communications Protocols CP-12 – Safe Mode CP-13 – Alternative Security Mechanisms	
[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] CSP should implement mechanisms to facilitate access to generally recognized international certificates, attestations and other applicable assessments in relation to organizational and technical controls regarding the Cloud Service. In this regard, note Controls [5.5.A], [5.5.B], [5.2.B] and respective Guidances. Addtionally, CSP can meet this requirement e.g. by providing copies, upon the Customer's request, of: ▪ one or more documents, including any document(s) made available to Customers online or incorporated by reference into the Cloud Services Agreement, comprising the list of technical and organisational measures taking into account the risks associated with the processing of Customer Personal Data, and/or, ▪ Current audit reports and/or certificates of compliance to ISO or other generally recognized international standards, especially in relation to information security, and/or ▪ Verified compliance with the EU Cloud Code of Conduct or any other recognized codes of conduct.		A.18 Compliance	A.18.1.1 Identification of applicable legislation and contractual requirements A.18.2.1 Independent review of information security	18.1 Compliance with legal and contractual requirements 18.2 Information security reviews A.10.11 Contract measures	6.15 Compliance	CC4.1 C1.1	UP-04 Certifications COM-02 Planning independent, external audits COM-03 Carrying out independent, external audits DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider	Access publicly available PDF version: NIST SP 800-53 3.13 PROGRAM MANAGEMENT PM-1 – Information Security Program Plan 3.1 ACCESS CONTROL AC-1 – Policies and Procedures 3.2 AWARENESS AND TRAINING AT-1 - Policies and Procedures 3.3 AUDIT AND ACCOUNTABILITY AU-1 – Policies and Procedures 3.4 ASSESSMENT, AUTHORIZATION, AND MONITORING CA-1 – Policies and Procedures 3.5 CONFIGURATION MANAGEMENT CM-1 - Policies and Procedures 3.6 CONTINGENCY PLANNING CP-1 - Policies and Procedures 3.7 IDENTIFICATION AND AUTHENTICATION IA-1 - Policies and Procedures	

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cybercurity Framework
									3.8 INCIDENT RESPONSE IR-1 - Policies and Procedures 3.9 MAINTENANCE MA-1 - Policies and Procedures 3.10 MEDIA PROTECTION MP-1 - Policies and Procedures 3.11 PHYSICAL AND ENVIRONMENTAL PROTECTION PE-1 - Policies and Procedures 3.12 PLANNING PL-1 - Policies and Procedures 3.14 PERSONNEL SECURITY PS-1 - Policies and Procedures 3.15 PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY PT-1 - Policies and Procedures 3.16 RISK ASSESSMENT RA-1 - Policies and Procedures 3.17 SYSTEM AND SERVICES ACQUISITION SA-1 - Policies and Procedures 3.18 SYSTEM AND COMMUNICATIONS PROTECTION SC-1 - Policies and Procedures 3.19 SYSTEM AND INFORMATION INTEGRITY	

Control	Control Guidance	GDPR	ISO 27001	ISO 27017	ISO 27018	ISO 27701	SOC 2	C5:2016	NIST SP 800-53	Cyberecurity Framework
									SI-1 - Policies and Procedures 3.20 SUPPLY CHAIN RISK MANAGEMENT SR-1 - Policies and Procedures CA-2 – Control Assessments SA-9 (1) – External System Services	