

# EU Cloud Code of Conduct



EU  
CLOUD  
COC

Version: 2.7  
Publication Date: June 2020  
Website: <https://eucoc.cloud>

**EU Data Protection Code of  
Conduct for Cloud Service  
Providers**

# 0 Contents

0	Contents	1
1	Introduction	2
2	Terminology	3
3	Structure of the Code	4
4	Scope	4
5	Data Protection	4
5.1	Terms and Conditions of the Cloud Services Agreement	4
5.2	Processing Personal Data Lawfully	5
5.3	Subprocessing	6
5.4	International Transfers of the Customers Personal Data	8
5.5	Right to audit	9
5.6	Liability	11
5.7	Cooperation with the Customer	11
5.8	Records of Processing	12
5.9	Data Protection Point of Contact	13
5.10	Rights of the data subject	13
5.11	Cooperation with the Supervisory Authorities	14
5.12	Confidentiality of the Processing	14
5.13	Assistance with Personal Data Breaches	15
5.14	Termination of the Cloud Services Agreement	16
6	Security Requirements	16
6.1	Security Requirements for CSPs under the Code	16
6.2	Detailed security objectives	17
6.3	Transparency	20
7	Monitoring and Compliance	20
7.1	Introduction	20
7.2	The Monitoring Body	20
7.3	Conditions of Adherence	22
7.4	Procedure to declare a Cloud Service adherent	22
7.5	Assessing compliance with the Code	23
7.6	Different Levels of Compliance and Compliance Marks	25
7.7	Monitoring and enforcement	26
7.8	Complaints Handling and Procedures	27
7.9	Sanctions, remedies and notification of the supervisory authority	28
8	Internal Governance	29
8.1	Organizational framework of the Code and its bodies	30
8.2	Code and guidelines	34
8.3	Finances	35
9	ANNEX A – Controls Catalogue	35

# 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<sup>1</sup> 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 extent 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,

<sup>1</sup> 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](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.
- **'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.

[5.1.E] CSP shall transparently communicate to Customers its adherence to the Code, at least as laid down in Section 7.6.3 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.

If the Cloud Services Agreement expressly authorizes the CSP or selected third parties engaged by the CSP or Customer to determine the purposes for which the Customer Personal Data are processed outside the context of the provision of the Cloud Services as specified in the Cloud Services Agreement, the CSP or such selected third party would be qualified as a controller or as a joint controller, and any such qualifications and related responsibilities must be clearly defined and allocated amongst the parties.

[5.1.H] The Cloud Services Agreement shall define the processing activities in relation to Customer Personal Data engaged in by the CSP and any sub-processors.

[5.1.I] Where the Customer expressly authorizes processing activities outside the provision of the Cloud Service , this shall be clearly defined and assigned contractually between the parties involved especially if creating joint-controllership.

## 5.2 Processing Personal Data Lawfully

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, taking into account Customer's own compliance requirements, the terms of the Cloud Services Agreement, and this

Code. The CSP shall always process Customer Personal Data according to Customers Instructions<sup>2</sup>.

[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.

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.

[5.2.H] 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.

### 5.3 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

<sup>2</sup> The CSP when acting as a processor shall therefore not process personal data except on documented instructions from the controller, unless required to do so by law, as specified in Article 28.3 GDPR.

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] 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

The Customer may itself transfer<sup>3</sup> 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.

[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 controls 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 data to a third country outside the EEA initiated by the CSP meet the requirements of GDPR, Chapter V.

[5.4.D] CSP shall continue to assess and monitor whether a country that is the destination of a data transfer under the Cloud Service Agreement is subject to an adequacy decision of the Commission.

[5.4.E] For data transfers with a destination that is outside the EEA the CSP shall document the specific safeguards under Chapter

<sup>3</sup> *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.

V GDPR a transfer is based upon and shall establish documented procedures to safeguard that no transfer of data takes place without appropriate safeguards in place.

CSP and Customer may be subject to conflicting, applicable laws. Applicability of laws may be result of different aspects, regardless being e.g. formal, material or just territorial.

A Code of Conduct is a voluntary tool developed by industry, whilst conflicts of laws are based on legislative frameworks and thus can only be resolved by regulators themselves. The Code acknowledges, though, that providing transparency in Cloud Service provision can be beneficial in this context. But as the circumstances under which conflicts of law may appear can be based on different reasons, the Code needs to leave the resolution up to the negotiation and agreement between Customer and CSP.

## 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<sup>4</sup> to provide evidence of compliance, in order to ensure that the Customer Audits

<sup>4</sup> 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.

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. 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.

### 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
- 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.

[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.

As potential future behaviours cannot be assessed ex ante, there are no controls. Compliance with this section is subject to assessment within the complaints handling and related procedures, Section 7.8.

## 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 (a copy of) 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 a copy of 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<sup>5</sup>, 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

<sup>5</sup> 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*

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 provided to the Customer and – where required by GDPR – competent supervisory authorities.

## 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).

[5.10.A] CSP shall establish documented procedures 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,

*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/news-room/document.cfm?doc\\_id=44100](http://ec.europa.eu/news-room/document.cfm?doc_id=44100), p.14.

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 responses 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.

### 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 (a copy of) the Customer Personal Data, stored by the CSP's Cloud Services and, upon expiry of the 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 a complete copy of 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 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, etc.).

[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<sup>6</sup>. 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

<sup>6</sup> 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

avoidance of doubt: it is not mandatory for a CSP to be certified against ISO 27001 / 27002.

[6.1.B] 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.C] 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.P] 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.P], it shall provide reasoning and evidence to the Monitoring Body why those measures adequately replace the Controls concerned.

## 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.

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.

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 0 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 may only suspend or revoke the appointment of the Monitoring Body for good cause, such as gross misconduct or fraud, or with a prior notification 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 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 appoint a new Monitoring Body within a grace period of 180 days, otherwise any verified declarations of adherence shall become void. If the intended new Monitoring Body lacks its accreditation pursuant to Article 41 GDPR, any verified declarations of adherence shall not become void if the aforementioned grace period will be exceeded only due to delays in the accreditation procedure of the competent supervisory authority and the Monitoring Body has submitted its application for accreditation to the competent supervisory authority within the grace period.

### 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 7.9.3), 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 7.9.4).

## 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 submit, for the Steering Board approval, its 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

CSPs 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 chooses 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 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, and Cloud Computing Compliance Controls Catalog (“C5”), 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.

### 7.5.4 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.

### 7.5.5 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.

Unless otherwise provided by the Code, 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: also, in cases, where a Cloud Service is delisted from the Public Register for whatever reason no Compliance Mark must not be used 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 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.

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.

### 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 should be able to reason its actions related to the manifestly unfounded or excessive character of the request.

### 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 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.

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 inevitable. Such a decision shall result into a review of the guidelines.

### 7.9.4 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;
- Approve Complaint Panel's guidelines submitted by the Monitoring Body, under the principle that the Complaint Panel (as described in Section 7.9.1.) shall be an independent body within the 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 7.9.3;
- 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.

### **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 –