EU Data Protection Code of Conduct for Cloud Service Providers

Version 2.0,
May 2018

EU
CLOUD
COC

Contents

Contents 1

Introduction 3

0. Terminology 5

1. Structure of the Code 6

2. Purpose 6

3. Scope 6

4. Conditions of Adherence 7

5. Data Protection 9

5.1. Contractual specification of the terms and conditions of the CSP's Cloud Services 9

5.2. Processing personal data lawfully 9

5.3. Subprocessing 10

5.4. International transfers of the Customer's personal data 11

5.4.1. Transfers on the basis of an adequacy decision 12

5.4.2. Transfers subject to appropriate safeguards 12

5.5. Right to audit 12

5.6. Liability 14

5.7. Cooperation with the Customer 14

5.8. Records of processing activities and nominating a privacy point of contact 15

5.9. Rights of the data subject 16

5.10. Cooperation with the data protection authorities 17

5.11. Confidentiality of the processing 17

5.12. Assistance with personal data breaches 17

5.13. Return and deletion of personal data 18

6. Compliance Controls and Security Requirements 19

6.1. Assessing compliance with the Code – the Controls Catalogue 19

6.2. Security requirements for CSPs under the Code – objectives and assessment 19

6.3. Detailed security objectives 20

Objective 1 - Management direction for information security 21

Objective 2 - Organisation of information security 21

Objective 3 - Human resources security 21

Objective 4 - Asset management 21

Objective 5 - Access controls 21

Objective 6 - Encryption 21

Objective 7 - Physical and environmental security 21

Objective 8 - Operational security 22

Objective 9 - Communications security 22

Objective 10 - System development and maintenance 22

Objective 11 - Suppliers 22

Objective 12 - Information security incident management 22

Objective 13 - Information security in business continuity 22

6.4 Transparency 22

7. Governance 23

7.1 Organizational framework of the Code and its bodies - governance bodies and administration 24

7.1.1. Code General Assembly 24

7.1.2. Code Supporter 26

7.1.3. Code Steering Board 26

7.1.4. Code Competent Monitoring Bodies 30

7.1.5. Code Secretariat 32

7.2. Members that have chosen to adhere to the Code 33

7.2.1. Procedure for self-assessment and self-declaration of adherence by Members 33

7.2.2. Complaints 33

7.2.3. Compliance Marks 34

7.2.4. Monitoring and enforcement 35

7.3. Code and guidelines 36

7.4. Finances 36

7.4.1. General 36

7.4.2. Secretariat 36

7.4.3. Monitoring Body 36

ANNEX A 38

Template declaration of adherence 38

A. Identification of the CSP 38

B. Contact information of the CSP's designated data protection officer(s): 38

C. Identification of the Competent Monitoring Body that verified this declaration of adherence 38

D. CSP Cloud Services covered by this declaration of adherence 38

E. Controllership with respect to the CSP services covered by this declaration of adherence 38

F. Third party certifications (if any) 38

ANNEX B 40

Checklist – step by step guidance to adherence to the Code of Conduct 40

ANNEX C 41

Controls Catalogue 41

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 cloud customers develop a level of confidence in a cloud service provider (CSP), before they entrust them with their data and applications. GDPR[1] requires that the customers, as the controllers of data, 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 Cloud Code of Conduct ("Code" or "Code of Conduct")[2] is to demonstrate these guarantees and make it easier and more transparent for cloud customers to analyse whether cloud services are appropriate for their use case. The transparency 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 cloud customers such as small and medium enterprises (SMEs) and public administrations.

The Code was created with "business-to-business" (B2B) cloud services in mind (where the CSP is typically acting only as a data processor to the cloud customer) and may not address all data protection issues arising in the context of "business-to-consumer" (B2C) services where the CSP may act as a data controller or where the cloud consumer may be covered by the household exemption[3].

The GDPR states that "*Member States, the supervisory authorities, the Board and the Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of GDPR, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises*" (Article 40). This Code of Conduct was initially prepared by the Cloud Select Industry Group (C-SIG) - Data Protection Code of Conduct Subgroup[4] which was convened by the European Commission (DG Connect and DG Justice). In February 2017 the Code was passed from the C-SIG to the new General Assembly of the EU Cloud Code of Conduct.

The Code consists of a set of requirements for CSPs and includes a Governance Section, which aims to support the effective and transparent implementation, management, and evolution

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

[2] This Code of Conduct has been prepared to contribute to the proper application of the GDPR, taking into account the specific features of the cloud computing sector.

[3] According to Article 2(2) of the GDPR, "This Regulation does not apply to the processing of personal data […] by a natural person in the course of a purely personal or household activity".

[4] See https://ec.europa.eu/digital-agenda/en/cloud-select-industry-group-code-conduct

of the Code, in accordance with the requirements of the GDPR. The Code is supported by a Controls Catalogue (Annex C), which helps CSPs to achieve and demonstrate compliance with the requirements of the Code. The Controls Catalogue maps the requirements of the Code to auditable elements, and furthermore maps the Code to the GDPR and relevant international standards, thus facilitating its application and interpretation in practice.

The Code is a voluntary instrument, allowing a CSP to evaluate and demonstrate its adherence to the Code's requirements. The Controls Catalogue should be used as an operational checklist to determine compliance.

Any CSP may sign up any or all of its service offerings to the Code, irrespective of where it is established or where the personal data is stored and processed, provided that the CSP meets all requirements of the Code. CSPs that have evaluated and demonstrated their adherence in accordance with the requirements in the Code may thereafter use the Code's Compliance Marks.

Prior to engaging a CSP on the basis of this Code, cloud customers are invited to verify that the CSP is listed on the website which enumerates all the companies involved in developing the Code and those that have declared Cloud Services adhering to this Code:

(https://eucoc.cloud/en/home/).

0. Terminology

Any terminology used in this Code of Conduct, 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.

Furthermore, the following defined terms[5] are used in this Code of Conduct:

- ‘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.
- ‘Cloud Service Provider’ or ‘CSP’: party which makes cloud services available.
- ‘Cloud Services Agreement’: a (set of) written agreement(s) 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.
- ‘Competent Monitoring Body’: means the accredited monitoring bodies, as provided in Article 41 do the GDPR, approved by the Steering Board.
- ‘Compliance Mark’: the declaration of compliance attributed to a declaration of adherence in accordance with Section 7 (Governance).
- ‘Customer’ or ‘Cloud Customer’: party which is in a business relationship for the purpose of using cloud services.
- ‘Customer’s Personal Data’: any personal data in relation to data subjects that the Customer, in its capacity as controller[6], entrusts to the CSP as part of the provision of the Cloud services.
- ‘Party’: natural person or legal person, whether or not incorporated, or a group of either.

[5] All definitions taken from ISO/IEC 17788 - Information technology — Cloud computing — Overview and vocabulary; see http://www.iso.org/iso/catalogue_detail?csnumber=60544, with the exception of the definitions of ‘Customer’s Personal Data’ and ‘Cloud Services Agreement’.

[6] The scope of this Code of Conduct includes scenarios, where the CSP acts as a subprocessor on behalf of another CSP who acts as a processor.

1. Structure of the Code

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

- **Purpose:** describes the ambitions of the Code and its relation to the GDPR.
- **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.
- **Conditions of adherence:** describes the conditions for CSPs declaring adherence to the Code, including particularly the Code’s relationship to the terms of Cloud Service that apply between the CSP and its Customers.
- **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 good security practices.
- **Governance:** describes how the Code is managed, applied and revised, including the roles and obligations of its governing bodies.

2. Purpose

The purpose of this Code is to provide trust and confidence to the Cloud Customers that the Customer’s Personal Data is processed with an appropriate level of data protection. 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 another processor).

When adhering to this Code, CSPs must commit to the Code's requirements and practices for the CSP’s Cloud Services to which the Code applies. In consequence, Cloud Customers should be more confident in the implementation by the CSP of the data protection rules. CSPs whose adherence to the Code has been published in the public register, in accordance with the Section 7 (Governance) of the Code, may choose to publicly show their adherence by using any of the Compliance Marks specified in accordance with Section 7 (Governance).

3. Scope

Any CSP may choose to declare its adherence to the Code, for any types of Cloud Services through which personal data may be processed.

It is not mandatory for the CSP to choose to declare the adherence of all of its Cloud Services to the Code. A CSP can choose to only declare specific Cloud Services as adherent to the Code. CSPs taking this approach will need to ensure that potential Customers are made unambiguously aware of which Cloud Services the Code applies to.

CSP Cloud Services may be listed individually or in combination with other CSP Cloud Services[7]. Where multiple Cloud Services are provided in combination, a Cloud Service may be provided by one CSP and supported by another. In order to try to simplify issues for the Customer, CSPs that are the sole contracting entity for a variety of Cloud Services provided should be the main point of contact for the Customer, and their contracts and related documents should provide Customers with needed information and disclosures related to the nested services as required under this Code. Where one CSP provides the Cloud Service and another is responsible for support or other related Cloud Services, this should also be made clear to Customers, including whom to contact for which issues. Where users 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. Customers should be provided with information necessary to enable them to understand the nature of the Cloud Service. Guidance is provided within the Code to help users of the Code 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 Service offerings in which personal data may be processed. However, the inclusion of all such Cloud Services in one Code will mean that not all Code provisions may be equally relevant to all Cloud Services.

4. Conditions of Adherence

By declaring its adherence to this Code of Conduct, the CSP commits to comply with the requirements of the Code for any Cloud Services covered by its declaration. Any declaration of adherence to the Code must relate to all parts of the Code: CSPs cannot declare to adhere to only a chosen part of the Code or to exclude certain Sections of the Code.

A declaration of adherence 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.

[7] E.g. via nested services, where a specific Cloud Service is built on top of other Cloud Services, possibly offered by a different CSP. A common example is a SaaS Cloud Service built using an IaaS service of another provider.

CSPs that meet the requirements set out in the Code may declare that they adhere to the Code, following the process outlined in Section 7 (Governance). CSPs that declare will undergo rigorous scrutiny by the Competent Monitoring Body, in compliance with Article 41 of the GDPR, according to the requirements of the respective Compliance Mark under which the Cloud Service is declared. This may vary, from a full self-assessment by the CSP verified by a plausibility check performed by the Competent Monitoring Body, to, at the other end of the scale, an assessment where the adherence to the Code is fully proven by independent third-party audits and certifications towards the Competent Monitoring Body.

Customers may consider the declaration of adherence for Cloud Services, covered by this Code provided by the Competent Monitoring Body, as made available in the public register before entrusting personal data to a Cloud Service Provider as sufficient guarantees under Article 28 of the GDPR.

For as long as a CSP declares adherence of a Cloud Service to the requirements of the Code, that CSP will ensure that key information, in relation to data protection compliance with regard to adhering Cloud Services, is made available to the Customer, as set out in this Code, including online and/or incorporated by reference into other contractual documents, and kept up to date. As a minimum, such information should include all elements covered by the Declaration of Adherence form in Annex A.

This Code was drafted to be fully consistent with the GDPR. Its application by any CSP should not result in any conflict with that CSP’s policies, procedures or standards. Any such conflict should be resolved before declaring adherence to this Code: CSPs should ensure that their legal or contractual obligations for Cloud Services covered by this Code do not contradict any part of the Code before declaring their adherence to its terms, and that their legal or contractual obligations for Cloud Services covered by this Code do not lower the level of data protection as provided by this Code. Customers of the CSP should ensure that the assurances of the Code in conjunction with any additional contractual assurances and their own policies are sufficient to meet their legal requirements.

It is the Customer's responsibility to consider and decide whether the Cloud Services offered by a CSP, adhering to this Code, are appropriate for the processing of its personal data. To facilitate the Customer's decision, CSPs shall appropriately inform the Customer with respect to the Cloud Services they are offering and the security measures in place, in accordance with the terms of the Code.

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 the Section 7 (Governance) of the Code.

5. Data Protection

5.1. Contractual specification of the terms and conditions of the CSP's Cloud Services

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, as highlighted in Section 4, the CSP shall ensure that the terms of its Cloud Services Agreement, which must contain all elements required under the GDPR, notably in Article 28.3, shall have at a minimum the same level of data protection obligations as provided for by this Code. Committing to compliance with the Code, as a mandatory term of the Cloud Services Agreement, satisfies this requirement. The CSP's standard Cloud Services Agreement templates must be consistent with the rights and obligations described in this Code before claiming adherence to the Code. The CSP should offer existing Customers the ability to incorporate the updated data protection terms into their Cloud Services Agreement.

The CSP and its Customer shall remain responsible for compliance with their respective obligations under GDPR, including in particular, 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 Section 7 (Governance) of the Code.

In its capacity as a processor, the CSP shall act only on behalf and under the documented instructions of the Customer, acting as a controller (or a processor), with respect to 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.

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's 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.

5.2. Processing personal data lawfully

The Customer remains responsible for complying with its obligations and duties under GDPR. The Customer remains responsible for verifying whether the CSP Cloud Services comply with the GDPR obligations applicable to Customer taking into account the terms of the Cloud Services Agreement and this Code. The CSP shall always follow the Customer's data processing documented instructions according to the provisions of the Cloud Services Agreement[8].

The CSP shall implement measures, as specified in the Cloud Services Agreement, which are designed to help satisfy, or if retention is managed by the Customer, which help enable the Customer to take steps to satisfy the requirements under GDPR that personal data processed pursuant to the Cloud Services Agreement will not be retained longer than necessary. The CSP shall make relevant elements of its data retention policy available to the Customer, in accordance with the Cloud Services Agreement.

If the CSP is not established in a Member State of the European Union but in scope of the GDPR by virtue of Art. 3.2, it must designate a representative in accordance with Article 27 of the GDPR, who must be established in one of the Member States where the data subjects, whose personal data are processed by the CSP, reside (or if this is unknown to the CSP, in one of the EU Member States where data processing occurs). The CSP shall grant the representative the authority to represent the CSP in particular towards supervisory authorities and/or data subjects, on all issues related to processing for the purposes of ensuring compliance with the GDPR.

5.3. Subprocessing

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

In accordance with Article 28.2 of the GDPR the CSP shall not engage a subprocessor without prior specific or general written authorization of or notice with opportunity to object to the Customer. The authorization or notice may be obtained in the Cloud Services Agreement. It may include provisions for the CSP to provide further processing activities involving changes of subprocessors or change in jurisdiction without the requirement to obtain additional authorization from the Customer.

The CSP shall notify the Customer in advance of any intended changes concerning an addition or a replacement of a subprocessor, engaged by the CSP based on a general authorization by the Customer, which provides processing activities on behalf of the Customer. 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 in the list on reasonable grounds or that would cause Customer to violate the GDPR. The CSP and the Customer may define in the Cloud Services Agreement in which cases an objection from the Customer to the use of a new subprocessor or jurisdiction would be

[8] 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 of GDPR.

unreasonable. If the Customer’s objection is found to be reasonable, and to the extent the CSP and the 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.

Where a CSP engages a subprocessor for carrying out specific processing activities on behalf of the Customer, the CSP shall, in accordance with Article 28.4 of the GDPR, ensure that the subprocessor provides at least an equivalent level of protection obligations, for instance providing sufficient guarantees that the subprocessor will implement appropriate technical and organizational measures in accordance with the requirements of the GDPR and as set out in the Cloud Services Agreement.

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.

Additionally, the CSP shall maintain an up-to-date list of subprocessors engaged by the CSP in the processing of the Customer’s personal data. The list should include the legal name of the subprocessor entity. Additionally, the CSP may describe in that list the function of each subprocessor.

For security reasons, the CSP may choose to only provide a general description of its subprocessor engagements to the Customer before entering into the Cloud Services Agreement with the Customer. This general description should allow the Customer to identify the country or countries where the data will be processed by the subprocessor and, whenever data are sent outside of the European Union, to inform the data subject.

Upon signature of the Cloud Services Agreement between the CSP and the Customer, disclosure of any additional information on the aforementioned list beyond the general description 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 data protection authorities upon their request.

5.4. International transfers of the Customer’s personal data

The Customer may itself transfer or provide instructions to the CSP to transfer, on its behalf, personal data to a third country outside the European Economic Area, as reflected in the Cloud Services Agreement.

Such international transfers shall take place only if the conditions in Chapter V of the GDPR are met. Meeting these conditions shall be a mutual responsibility of the CSP and the Customer, specifically if the entity receiving the data in the third country is not a third party but the CSP itself or subprocessor engaged by the CSP.

5.4.1. Transfers on the basis of an adequacy decision

If the third country in question is subject[9] to an adequacy finding by the Commission pursuant to Article 45 of the GDPR, the transfer may take place without any specific authorization or additional safeguards.

The adequacy decision in relation to the United States is limited to the EU-US Privacy Shield framework and only extends to entities in the United States that have self-certified adherence to the Privacy Shield Principles[10] to the US Department of Commerce. The Privacy Shield benefits are assured from the date on which the US Department of Commerce has placed the entity's self-certification submission on the Privacy Shield List, after having determined that the submission is complete.

5.4.2. Transfers subject to appropriate safeguards

In the absence of an adequacy decision mentioned in Section 5.4.1. above, a CSP or Customer may transfer personal data to a third country if the receiving entity in the third country, such as the CSP or the CSPs subprocessor, provides appropriate safeguards and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The appropriate safeguards referred to above may include:

- Binding corporate rules, in accordance with Article 47 of the GDPR;
- Standard data protection clauses, approved by the Commission in accordance with Article 93.2 of the GDPR;
- An approved code of conduct, pursuant to Article 40 of the GDPR, together with binding and enforceable commitments of the processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;
- An approved certification mechanism, pursuant to Article 42 of the GDPR, together with binding and enforceable commitments of the processor, in the third country, to apply the appropriate safeguards, including as regards data subjects' rights.

A CSP who is a recipient of an international transfer by the Customer or transfers data to subprocessors in third countries, under the instruction of the Customer, shall make it clear in the Service Agreement how it assists the Customer in complying with the conditions in Chapter V of the GDPR.

5.5. Right to audit

The Customer must be able to assess whether the CSP complies with its obligations under the Code, and under GDPR as a processor. This Code ensures that compliance can be assessed by

[9] See https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en for a current list of destinations that satisfy the requirements.

[10] See https://www.privacyshield.gov/EU-US-Framework

the Customer, through the review of any available independent third-party audit reports provided by the CSP, or, exceptionally and under the conditions stated below, by audits conducted by the Customer under the terms of its Cloud Services Agreement.

In either case, the CSP must provide appropriate evidence to the Customer with respect to compliance, when required in accordance with this Section 5.5. These audit rights ensured by the Code do not affect the competence of data protection authorities to monitor compliance with GDPR in accordance with their legal mandate.

If the CSP, or the relevant Cloud Service, has not received information necessary to demonstrate compliance, then the CSP acting as a processor on behalf of the Customer shall (a) permit the Customer to request an audit, by a mutually agreed auditor, that is bound by a written confidentiality agreement or obligation or (b) allow the Customer to conduct such an audit, provided that, in both cases, this right has been granted to the Customer through the Cloud Services Agreement or the Customer demonstrates the need for such an audit in light of its respective applicable GDPR requirements as the controller of personal data.

If the CSP or the relevant Cloud Service has received certificates, attestations, or reports resulting from accredited independent third-party audits, such as ISO 27001, SSAE SOC 2, approved codes of conduct under the GDPR and other industry standards, these are presumed to meet the general audit requirements of the Customer in the field of data protection and security. However, the Cloud Service Agreement shall permit the Customer the ability to gain additional evidence of compliance of any specific instructions provided to the CSP to the extent the above-mentioned certificates, attestations, or reports do not fully address the scope of the audit request made by the Customer.

Upon request, in accordance with the Cloud Services Agreement, the CSP shall provide to Customers, free of charge, a summary report describing the outcomes of any audits conducted for the purposes of obtaining a Certificate in accordance with the Code. The summary report shall contain a sufficient description of the CSP's compliance controls to provide the Customer with assurance that the CSP has complied with its obligations as a processor under GDPR; the CSP may exclude confidential information that would endanger the security and protection of data, including personal data, in the CSP infrastructure.

The CSP may maintain reasonable protocols for audits, such as requiring the Customer to provide written notice reasonably in advance of the proposed audit date, carrying out any audits during regular business hours in a way not to be disruptive to normal business operations, and setting forth a defined scope for a mutually agreed audit plan in accordance with the Cloud Services Agreement[11]. The CSP and the Customer may specify any arrangements in relation to the cost allocation for audits in the Cloud Services Agreement. In

[11] In emergency or crisis situations audits may not always allow as much notice or consideration of business operations as desired.

the absence of any arrangements in relation to the costs and cost allocation, the costs must be borne by the requesting party.

Upon completion of an audit, the parties shall exchange a copy of the audit report, which shall be treated as confidential information pursuant to the terms of the Cloud Services Agreement. To the extent feasible, the CSP shall provide Customers with self-service access to any independent third-party audit reports or enable self-service mechanisms for ongoing monitoring. For example, the CSP may provide for the ability for the Customer to verify the Customer’s datacentre region online, or to view current lists of subprocessors through a self-service mechanism.

Onsite visits to datacentres introduces a potential security risk for all other Customers of the CSP, whose data is hosted within the same premises or facilities. The CSP can limit onsite visits of the facilities used to provide the Cloud Service if the above information does not satisfy an audit obligation mandated by the GDPR, and Customer can provide response as to why the independent audits cannot fulfil their audit obligations. If an onsite audit is absolutely necessary, it shall be conducted in a manner that a) minimizes risk of disruption to CSP's business and clients, b) is in conformity with the CSP's practices, policies and legal obligations, and c) does not violate agreements, rights or legal obligations of other subscribers or their data subjects.

5.6. Liability

Where the CSP has acted outside or contrary to lawful instructions of the controller, 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 the GDPR. As part of the liability regime, the CSP and the Customer shall specify any applicable liabilities for subprocessors.

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

5.7. Cooperation with the Customer

The CSP shall reasonably assist the Customer with certain obligations, as specified under Article 28 of the GDPR. In the event that a Customer receives a data subject access request for personal data processed by the CSP, a CSP adhering to the Code may support the Customer in responding to such requests by (1) providing the Customer with ability for the Customer to gather the data themselves, via the Cloud Services provided by the CSP, and/or (2) providing additional reasonable assistance in gathering the requested data, to the extent such data is not accessible to the Customer.

The CSP shall provide a mechanism that may support the Customer with any questions or requests it may have regarding the data protection measures covered by both the Cloud Services Agreement and this Code. Such mechanisms 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 privacy point of contact as described in Section 5.8. below.

Furthermore, the CSP shall reasonably assist the Customer in completing any data protection impact assessments required under GDPR. The CSP may charge a fee for customized assistance under the Cloud Services Agreement. Such assistance shall require the CSP to cooperate in good faith with the Customer (1) to provide information about Cloud Services provided, which is reasonably needed by the Customer, and reasonably available to the CSP given the nature of the Cloud Service, (2) to enable the evaluation of risks to the data protection rights of data subjects and (3) in the determination of appropriate technical and organizational measures to be implemented by the CSP, taking into account the purposes for which the Customer will use the CSP's Cloud Services as determined in the Cloud Services Agreement. If such information is confidential or otherwise sensitive, the CSP may require the Customer to execute a confidentiality agreement, which is acceptable to the CSP. The confidential information may be excluded to the extent that it would pose a risk to the security or privacy of the data processed by the CSP.

Finally, if the CSP supports the possibility for the Customer to retrieve (a copy of) the personal data that it has entrusted to the CSP, the CSP will inform the Customer in a sufficiently detailed, clear and transparent manner about the processes, technical requirements, timeframes and any charges that apply if the Customer wants to obtain any personal data that it provided to the CSP. Specifically, the CSP must at least inform the Customer regarding the available data formats, transfer mechanisms and transfer characteristics, required configuration at the Customer's side, and typical timeframes.

The CSP may provide such assistance in the form of standard documentation or audit reports available to all Customers and may also charge a fee for additional customized assistance under the Cloud Services Agreement.

5.8. Records of processing activities and nominating a privacy point of contact

The CSP shall maintain written records of its processing activities that comply with the requirements of Article 30.2 of the 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;

- Where applicable, transfers of personal data to a third country and the underlying documentation of suitable legal safeguards to secure the transfer;
- Where possible, a general description of the technical and organisational security measures.

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

Furthermore, CSPs adhering to the Code shall nominate a data protection officer, when required under the GDPR, or, as a minimum, the CSPs shall have a privacy team[12], meeting the requirements of Chapter IV, Section 4 of the GDPR, who shall perform the functions defined in the GDPR in relation to any Cloud Services covered by its declaration of adherence. The CSP will ensure that such a data protection officer or privacy team 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.

5.9. 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, typically the Customer, 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).

The CSP shall ensure that its designated data protection officer or privacy team are easily reachable by Customers.

Depending on the information available to the CSP and the nature of the Cloud Service, and provided the Customer doesn't have the ability to do so, the CSP shall cooperate with the Customer to help the Customer to address any reasonable data subject rights requests made by a data subject to the Customer for access, rectification or erasure, complaints, the right to data portability, the right to restriction of processing or any implementation of data subject rights in a timely and efficient manner.

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

5.10. Cooperation with the data protection authorities

Depending on the information available to the CSP and the nature of the cloud service provided:

- The CSP shall cooperate in good faith with the Customer and provide reasonable assistance to the Customer to enable the latter to handle a request from a competent data protection authority regarding the processing of the Customer's personal data, as part of the Cloud Service.
- The CSP shall cooperate in good faith in response to all data protection authority requests it receives directly, in particular to ensure adequate and timely responses. The CSP will notify the Customer, where appropriate under the circumstances, of any such requests received from a data protection authority that relate to the processing of the Customer's personal data under the Cloud Services Agreement, unless such notifications are not permitted under applicable law.

5.11. Confidentiality of the processing

The CSP shall ensure that any personnel involved in the processing of the Customer's 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 aware of their obligation to respect the confidentiality of the personal data, as described within the terms of, for example, the employment agreement or confidentiality agreement.

Such persons shall specifically not be permitted to collect, use or otherwise process 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.

The CSP shall in addition ensure that personnel having access to the Customer's personal data shall be required to undergo appropriate training.

5.12. 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, 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 of 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 description in the Cloud Service Agreement of the technical and organisational security measures, put in place by the CSP, shall contain measures that enable the CSP to detect, address and report a breach of security in a timely manner.

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. Return and deletion of personal data

Depending on the information available to the CSP and the nature of the Cloud Service provided, where the CSP has access to the Customer personal data, the CSP shall enable the Customer's choice after the end of the provision of the services under the Service Agreement:

- To receive (a copy of) the Customer's personal data, stored by the CSP's Cloud Services and, upon expiry of the designated period for Customer to retrieve its personal data, subsequently delete the relevant personal data; or
- To delete the Customer's personal data stored.

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 personal data to another CSP.

The CSP will not be required to ensure that the return of the personal data remains possible after the termination of the Cloud Services Agreement, unless otherwise agreed in the Cloud Services Agreement.

After the termination of the Cloud Services Agreement, or upon expiry of the designated period for the Customer to retrieve its personal data, the CSP shall delete any remaining copies of the Customer's personal data within the timescale specified in the Cloud Services Agreement or (if no timescale was specified in the Cloud Services Agreement) no later than one year after the termination of 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.).

6. Compliance Controls and Security Requirements

6.1. Assessing compliance with the Code – the Controls Catalogue

In order to ensure that the Code's monitoring bodies and data protection authorities can verify that requirements of this Code are adhered to by CSPs, where appropriate the requirements of this Code have been mapped into a catalogue (described in Annex C). Referred to as the Controls Catalogue, this is made available to CSP’s that sign up to this code. While the Code is a standalone document that contains all requirements for adherence, the Controls Catalogue should be understood as an operational document that allows CSPs and third parties to determine more easily, in practice, if they indeed meet all requirements.

In a practical sense, the Controls Catalogue can be considered a check list, containing each clause of the Code that implies an obligation to be verified, and provides implementation and control guidance (how should the obligation be interpreted and assessed in practice), along with a mapping to the corresponding provision of the GDPR (article and paragraph), and references to other standards or schemes, including ISO 27001, ISO 27018, SOC 2 (2017TSC), and C5.

The Controls Catalogue does not overrule any part of the Code, nor does it imply that compliance with the referenced standards or schemes would be sufficient, as such, to show compliance to the Code or to the GDPR. The Controls Catalogue specifies the provisions of the Code and has binding character towards CSPs adherent to the Code and third parties, including the Competent Monitoring Body, when assessing CSPs. The Controls Catalogue should be understood as a tool that allows CSPs or third parties to assess consistently which controls are required in practice, including in cases where an existing certification is already in place, which might cover all or part of any given requirement. The objective is therefore to establish an objective assessment tool, for the benefit of CSPs, the governance of the Code, and verifications by third parties including DPAs.

The Controls Catalogue is not a static document: it is intended to be maintained, e.g. by adding additional standards or schemes, or by clarifying the existing implementation and control guidance.

6.2. Security requirements for CSPs under the Code – objectives and assessment

In accordance with the requirements of the GDPR, both controllers and processors (and thus also including CSPs acting as processors) must 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.

For CSPs, many of these elements are hard to appreciate in practice, since a CSP's actual knowledge of the personal data being processed via their Cloud Services and the related risk may be very limited or very detailed depending on the Cloud Service. Nonetheless, it is important to recognize that CSPs have an obligation to implement measures ensuring an appropriate level of security in light of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

The nature of the technical and organizational information security measures implemented by the CSP shall take into account the CSP's knowledge (if any) of the sensitivity of the personal data being processed, including by considering the nature of the Cloud Service, and the impact of any personal data breach, both on the data subjects and on the Cloud Service Customer, insofar as this is known to the CSP[13]. Where the CSP offers a Cloud Service, which could be used to process 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.

Since it is not possible to define security requirements that are necessary or suitable for all types of Cloud Services, the Code requires a clear and explicit application of the accountability principle of the GDPR: CSPs that wish to adhere to the Code must assess, for the Cloud Service covered, whether certain security objectives can be achieved, and if so, how. The controls are summarily listed below and elaborated upon in greater detail in the Controls Catalogue.

6.3. 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 ISO27001, SOC, C5 and so forth. In addition, CSPs should demonstrate compliance with GDPR specific requirements, as further elaborated 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 CSP's.

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

Objective 1 - Management direction for information security

The CSP shall have clear management-level direction and support for the security of Cloud Service Customers' personal data processed by the CSPs Cloud Services.

The CSP shall have in place a management-approved set of information security policies that govern the security of Cloud Services Customers' personal data in the CSPs Cloud Services.

Objective 2 - Organisation of information security

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

Objective 3 - Human resources security

The CSP shall take all reasonable steps to ensure that all employees, contractors and other individuals, within the CSPs control, who have access to Customers' 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.

Objective 4 - Asset management

The CSP shall take all reasonable steps to ensure the security and confidentiality of the CSPs assets and facilities associated with the processing of Customers' data, with policies for deleting or rendering personal data unrecoverable.

Objective 5 - Access controls

The CSP shall limit access to Customers' personal data, both in the cloud and the facilities in which the Customers' personal data is processed, including through logical access controls.

Objective 6 - Encryption

Where technically and commercially 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 Customers' personal data in the cloud, where provided for in the Cloud Services Agreement or where considered necessary based on a risk analysis.

Objective 7 - Physical and environmental security

The CSP shall adopt physical and environmental security measures, designed to prevent unauthorized access, alternation to or destruction of Customers' personal data in the cloud and to the related information processing facilities.

Objective 8 - Operational security

To the extent the CSP is responsible for the Customer's personal data in the operations of the Cloud Service, the CSP shall take all reasonable steps to ensure the secure operation of facilities and services that are involved in the CSP's processing of a cloud Customer's 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 Customers' personal data security.

Objective 9 - Communications security

The CSP shall take all reasonable steps designed to ensure the protection of Cloud Services Customers' 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.

Objective 10 - System development and maintenance

The CSP shall take all reasonable 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 Customers' personal data.

Objective 11 - Suppliers

The CSP shall take all reasonable steps to ensure that Customers' personal data is adequately protected where the CSP's subprocessors have access to the CSP's cloud systems or assets.

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.

Objective 13 - Information security in business continuity

To the extent the CSP is responsible for the Customer's personal data in the operations of the Cloud Service, the CSP shall take all reasonable steps to ensure that information security continuity, with respect to Customers' 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 Customers' personal data in adverse situations, e.g., a disaster.

6.4 Transparency

The CSP should describe the level of security provided by the CSP to protect Customers personal data processed by the CSP as part of the Cloud Services by providing appropriate information about the technical and organizational measures it has in place.

The CSP should also provide the Customer with up-to-date information, with an appropriate level of detail, about the technical and organisational measures that are in place.

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.
- Current audit reports and/or certificates of compliance to ISO or other generally recognized international standards, especially in relation to information security.
- Certificate of compliance with the EU Cloud Code of Conduct or any other recognized codes of conduct.

However, the Cloud Service Provider shall not be required to disclose any business confidential or commercially sensitive information to the Customer. Furthermore, CSP disclosures must not be of a nature that could be used to compromise system security or integrity.

7. 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, a Secretariat for administrative support and Competent Monitoring Bodies to facilitate monitoring and enforcement. This includes rules for the composition, recognition, tasks and oversight of all of these bodies.
- Secondly, the governance of the CSPs that have chosen to adhere to the Code. This includes rules in relation to the publication of a list of adhering CSPs, certification of CSP Cloud Services, the use of Compliance Marks and mechanisms for monitoring and enforcement.
- Thirdly, 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.

7.1 Organizational framework of the Code and its bodies - governance bodies and administration

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

7.1.1. Code General Assembly

(a) **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.

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.

(b) **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 the Competent Monitoring Bodies accounts; to approve annual membership fees, Supporter fees and any other fees as proposed by the Steering Board; to approve new Members; to decide on the suspension or exclusion of any Member; to approve changes to the Code, and to decide on any other matters as requested by the Steering Board.

(c) **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.

(d) **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 Code Secretariat.
- The Chairman shall convene one annual General Assembly, during the first quarter of each civil year, to approve at least the Monitoring Body's accounts and 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 Competent 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.

(e) **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.

(f) **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.

7.1.2. Code Supporter

Separate from the General Assembly, and without obtaining membership or 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, data protection authorities, academia, or consultancy organisations) may request Code Supporter status.

All Code Supporters will be required to pay the annual Supporter membership fee, as set out by the General Assembly. Existing Supporters will be published on the Code website. Supporter status is terminated automatically when the Supporter chooses not to renew.

7.1.3. Code Steering Board

(a) **Composition**

Unless otherwise agreed by a decision of the General Assembly, 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 Code Steering Board includes representatives of:

- Cloud service providers 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 Code Steering Board may decide to appoint a drafting team of qualified experts to prepare amendments to the Code.

(b) **Powers**

The Code 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 Competent Monitoring Bodies, define and propose the content of the Code declaration of adherence and any guidelines for self-assessment;
- In consultation with the Competent Monitoring Bodies. define and propose minimum requirements for the assessment of those declarations of adherence by a Competent Monitoring Body;
- Approve Complaint Panel's guidelines submitted by the Competent Monitoring Body, under the principle that the Complaint Panel (as described in Section 7.1.4.) shall be independent;
- Define and propose guidelines for Code certification by auditors, specifically in order to identify appropriate existing standards and certification schemes that can be used to confirm compliance with all or parts of the Code. Within such guidelines, 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 in relation to security requirements, or for specific use cases, data types, service provisioning models, sectors or industries; such guidelines may however never lower the level of data protection as provided by the present Code, and will, at all times, ensure compliance with the GDPR;
- 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;
- Approve Competent Monitoring Bodies and withdraw or suspend an approval in case of factual indications that a Competent Monitoring Body no longer meets the requirements defined in this Code; A Competent Monitoring Body shall only be approved by the Steering Board, after the Steering Board has determined that the

Competent Monitoring Body is capable of performing the functions referred in Section 7.1.4. below, 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 apply the Code; to monitor their compliance with the Code's provisions, and to periodically review the Members operation if needed;

- Approve the Code Secretariat, selecting a suitable organisation to perform the Code Secretariat tasks on the basis of non-discriminatory and objective criteria;
- Approve any external third-party auditors;
- Discuss and submit for the approval of the General Assembly, membership fees, Code Supporters fees and, in consultation with approved Competent Monitoring Bodies, fees for declaration of adherences and their reviews, complaints fees, and any other fee that might be applicable;
- Propose, in consultation with the Competent Monitoring Bodies, for the approval of the General Assembly, the allocation of a share of the annual membership fees, from Members that have signed a declaration of adherence, to safeguard the Competent Monitoring Bodies' legal minimum functionality and independence (Section 7.4.3.);
- Define the appropriate actions in case of an infringement of the Code or in case a Member is not providing the information necessary to review a possible infringement of the Code to a Competent Monitoring Body;
- Propose, for the decision of the General Assembly, the applicable sanctions in case of an infringement of the Code, such as suspension or exclusion from the Code, and the publication of decisions in relation thereto;
- 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.

(c) **Board**

The Code 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 7.1.3. (a) Composition above;

- 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.

(d) **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 Code 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.

(e) **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.

(f) **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.

(g) **Disputes**

The Code Steering Board shall develop appropriate policies to assure that interests are disclosed, and conflicts are avoided. Mechanisms will include separation of duties, recusal or other policies undertaken by the Code Steering Board, and possibilities for the General Assembly to raise objections against individual Steering Board members. The Code 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.

7.1.4. Code Competent Monitoring Bodies

(a) Code Competent Monitoring Bodies, accredited in accordance with Article 41 of the GDPR shall perform the following functions:

- Review and approve declarations of adherence by Members;
- Regularly monitor whether the operations of the Members are in accordance with the Code;
- Review and decide complaints about infringements of the Code;
- 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 Members, and transparently communicates these procedures and structures;
- Implement procedures and structures that prevent conflicts of interests;
- Take appropriate action, selecting from among the sanctions as defined by the Steering Board, against a Member in case of an infringement of the Code or in case a Member is not providing the information necessary to review a possible infringement of the Code to a Competent Monitoring Body;
- Inform the competent supervisory authority of final actions taken against Members and the reasons for taking them.

(b) Competent Monitoring Bodies shall develop and implement appropriate policies, procedures and structures to:

- Ensure independence and expertise in relation to the Code, for instance a minimum period of appointment, limitation of expulsion to cause and expertise of its personnel and of the members of the Complaint's Panel;
- Allow approval of declarations of adherence by Members and to regularly monitor whether the operations of the Members are in accordance with the Code;
- Handle complaints about infringement of the Code or the manner in which the Code has been or in being implemented by each Member, including by appointing an independent Complaints Panel and submitting, for the Steering Board approval, the Complaints Panel guidelines;
- Ensure internal separation of duties within its structures, and within the body, the Members and members of the Complaints Panel (which is an independent body), and prevent conflicts of interest, implementing, for example, safeguards that different complaints, 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 provisions of the Code within a reasonable period of time;
- Ensure that expertise of individuals working for Competent Monitoring Body, including members of the Complaints Panel is proven by relevant academic degrees, several years of relevant working experience and/or relevant publications.

Competent Monitoring Bodies shall make the referred policies, procedures and structures public and available to Members and Customers, by always disclosing them in their website.

(c) Under the GDPR, Article 41, only bodies which are accredited as a monitoring body can apply for a Steering Board approval as a Competent Monitoring Body. Bodies, which were already approved as Code Competent Monitoring Body by the Steering Board before the GDPR has entered into force, will be obliged to apply for an accreditation pursuant to Article 41 of the GDPR within a reasonable timeframe. In case the accreditation decision is not made within reasonable time or the accreditation is finally rejected, the Code of Conduct Steering Board shall suspend or revoke the approval of the body. Multiple Competent Monitoring Bodies may be approved, in accordance with Article 41 of the GDPR, if structures and procedures are implemented that appropriately safeguard each Monitoring Bodies independence, coherent actions and decisions within such multitude of Monitoring Bodies.

(d) The Competent Monitoring Bodies are allowed to use the information obtained during a review process only for purposes related to its responsibilities pursuant to the Code. Each Competent Monitoring Body, as applicable, 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.

(e) Any decision or action taken by a Competent 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 at least for three years. Any further details may be governed by specific procedures of the Competent Monitoring Body.

(f) Upon reasonable request of a Competent Monitoring Body and in accordance with its duties and competencies under the Code, Members are under the obligation to cooperate with any Competent Monitoring Body with respect to providing information to the Competent Monitoring Body. Breach of such obligation could amount to an infringement of the Code.

7.1.5. Code Secretariat

(a) The Code Secretariat performs the following functions:

- Maintain a public register of Code Competent Monitoring Bodies;
- Maintain a public register of declarations of adherence by Members;
- Maintain a public register of certificates;
- 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.

7.2. Members that have chosen to adhere to the Code

7.2.1. Procedure for self-assessment and self-declaration of adherence by Members

Members submit their declaration of adherence in accordance with Annex A to a Code Competent Monitoring Body[14] listed in the public register, along with any additional information that may be required under the guidelines established by the Steering Board.

Upon reasonable request by the Competent Monitoring Body, the Member shall provide information relevant for the declaration of adherence in an up-to-date and accurate manner.

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

- Cloud Service adherent to the Code;
- Date of declaration of adherence approval;
- Level of compliance (Compliance Mark);
- Report of the declaration of adherence approval by the Competent Monitoring Body;
- Due date of the declaration of adherence.

The Member is then entitled to use the declaration of adherence and the Compliance Mark as described in Section 7.2.3. below.

A Member whose declaration of adherence has been rejected by a Competent Monitoring Body may submit a revised request of declaration of adherence or file a complaint.

7.2.2. Complaints

(a) **Complaints of Members against decisions of any Competent Monitoring Body**

Members may file a complaint against any decision taken by either a Competent Monitoring Body.

Complaints against any rejection of the approval of a declaration of adherence or certification shall be addressed to the competent independent Complaints Panel. The independent Complaints Panel decides on the validity of a declaration of adherence based on the information presented to the Competent Monitoring Body.

(b) **Complaints against any Member and its Cloud Services' declaration of adherence**

[14] Or to the European Steering Board, until a Competent Monitoring Body is appointed.

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

If no such solution can be found, the Customer can submit a complaint to the Competent Monitoring Body that reviewed and approved the respective declaration of adherence or issued the respective certificate.

The Competent Monitoring Body shall review the complaint, require the Member to provide any relevant information for the purposes of fact finding, and initiate a complaint handling process, in which the Complaints Panel will take decisions to solve such disputes.

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 Complaints Panel guidelines previously approved by the Steering Board. Complaints Panel members will be appointed by the Competent Monitoring Body.

7.2.3. Compliance Marks

(a) **Entitlement to use Compliance Marks**

Any Member that has been duly registered in the Code's public register is entitled to use the applicable Compliance Mark.

Should a dispute concerning non-compliance arises, a Member is entitled to continue using the Compliance Mark. After receiving a final finding of non-compliance with the Code, that Member must immediately cease to use the Compliance Mark.

The Code considers different levels of Compliance Marks in order to provide transparency to the Customers on the Cloud Services adherence choices.

The Code provides three different levels of compliance:

First Level of Compliance

The Member has performed a self-assessment and self-declaration of adherence to the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the provisions set out in this Code and further specified in the Controls Catalogue. The Competent Monitoring Body verifies that the Cloud Service complies with the Code through a plausibility check.

Second Level of Compliance

The Member has performed a self-assessment and self-declaration of adherence to the Code with regard to the declared Cloud Service and confirms that the Cloud Service fully complies with the provisions set out in this Code and further specified in the Controls Catalogue. The Competent Monitoring Body verifies that the Cloud Service complies with the Code. Where no certification is available, a plausibility check will be conducted.

Compliance with the Code is partially supported by independent third-party certificates and audits, which the Member has undergone with regard to this Cloud Service. Any such third-party certificates and audits that were considered to be relevant by the Competent Monitoring Body shall be cited in the report of the approval by the Competent Monitoring Body. Members must notify the Competent Monitoring Body if there are any changes to the provided certificates or audits.

Third Level of Compliance

The Member has performed a self-assessment and self-declaration of adherence to the Code with regard to the declared Cloud Service and confirms that Cloud Service fully complies with the provisions set out in this Code and further specified in the Controls Catalogue. The Competent Monitoring Body verifies that the Cloud Service complies with the Code. Compliance with the Code is fully supported by independent third-party certificates and audits the Member has undergone with regard to the Cloud Service. Any such third-party certificates and audits that were considered to be relevant by the Competent Monitoring Body shall be cited in the report of the approval by the Competent Monitoring Body. Members must notify the Competent Monitoring Body if there are any changes to the cited certificates or audits. The Controls Catalogue may give guidance on third party certificates that are regarded to be adequate in terms of complying with the Code.

7.2.4. Monitoring and enforcement

(a) **Monitoring**

The compliance of any Member that has declared its adherence to the Code will be monitored by a Competent Monitoring Body as noted above.

Any declaration of adherence shall be reviewed every twelve months unless any significant changes occur to the declaration adherence to the Code, in which case they shall be reviewed earlier. Each individual annual revision does not need to cover all provisions of the Code; however, over successive reviews, all provisions of the Code will be covered.

The Competent Monitoring Body shall perform additional reviews, as appropriate. This may arise in the case of a customer complaint, an adverse media report or anonymous feedback about a CSP which has declared a service adherent to the Code.

(b) **Enforcement**

If a Competent Monitoring Body becomes aware of any non-compliance of an adherent Cloud Service, the Competent Monitoring Body can request the Member to take specific measures to make that Cloud Service become compliant with the Code. In consultation with the Complaints Panel, the Competent Monitoring Body shall take the appropriate action with regards to the possible sanctions and remedies in accordance with the Complaints Panel guidelines approved by the Steering Board.

In the event that a declaration of adherence is revoked, the Code Secretariat shall delete that particular Cloud Service from the public register. The Member shall cease to make reference to the Code or the Compliance Mark in any of its documentation or publications, including its website.

7.3. 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 a Competent Monitoring Body.

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

The Code General Assembly shall submit the revised Code for endorsement in accordance with Article 40 of the GDPR. Comments from the supervisory authorities and the European Data Protection Board should be incorporated as appropriate, approved by the Code General Assembly and published.

7.4. Finances

7.4.1. General

The costs for the Code of Conduct Secretariat and the Code of Conduct Monitoring Bodies should be covered by fees raised by its Members and Supporters.

All costs of the Code of Conduct Secretariat and the Code of Conduct Monitoring Bodies and fees are publicly available.

7.4.2. Secretariat

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

7.4.3. Monitoring Body

Fees that Members pay to obtain the approval of a declaration of adherence shall be allocated to cover the operating costs of the Competent Monitoring Bodies, as decided. The fees apply regardless of the outcome of the declaration of adherence process. The fees shall not vary between different Competent Monitoring Bodies.

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

The Competent Monitoring Bodies must present their financial records to the Steering Board until January of each year, which submit them to the approval of the General Assembly.

Complaints may be subject to fees, which shall be cost-based and approved by the General Assembly.

ANNEX A

Template declaration of adherence

Through this declaration of adherence, the CSP identified below formally declares that all information contained herein is truthful, accurate, complete and up to date, and that all Cloud Services, as identified in this declaration adhere to all relevant parts of the Code of Conduct. The CSP will ensure that the information will be updated as necessary to ensure its continued truthfulness, accuracy and completeness.

A. Identification of the CSP

[Name, legal form, head office, share capital, place of registration, VAT number]

B. Contact information of the CSP's designated data protection officer(s):

[e-mail address of the designated DPO(s)]

C. Identification of the Competent Monitoring Body that verified this declaration of adherence

[SCOPE Europe SPRL, established at Rue de la Science 14, 1040 Brussels, Belgium]

D. CSP Cloud Services covered by this declaration of adherence

- E.g., Service (family) 1: Commercial name, summary free form description
- E.g., Service (family) 2: Commercial name, summary free form description
- Etc.

E. Controllership with respect to the CSP services covered by this declaration of adherence

For all the CSP Cloud Services covered by this declaration of adherence (tick only one option):

- The CSP declares itself to be the controller for at least some purposes, and affirms that it is complying with the related legal obligations;
- The CSP does not declare itself to be the controller for any of the purposes of processing.

F. Third party certifications (if any)

All CSP Cloud Services covered by this declaration of adherence has undergone the following certifications in the last 12 (twelve) months prior to submitting this declaration of adherence, and undergo re-certification (to be specified for each certification):

- [Standard 1 against which compliance is assessed] – [Name of accrediting body, legal form, seat of establishment]
- [Standard 2 against which compliance is assessed] – [Name of accrediting body, legal form, seat of establishment]
- Etc.

ANNEX B

Checklist – step by step guidance to adherence to the Code of Conduct

A CSP seeking to declare its compliance with the Code should undergo the following steps:

- Review the Cloud Services Agreement (including any terms and conditions or privacy policies) in relation to any Cloud Services for which a declaration of adherence is desired, in order to ensure that they do not conflict with the terms of the Code;
- Ensure that it provides all necessary information to prospective Customers prior to the conclusion of the Cloud Services Agreement, to allow them to make an informed decision on the suitability of the CSP Cloud Services for the purposes envisaged by the Customer;
- If data transfers are contemplated to subprocessors, the CSP should ensure that the demonstration keys specified by the Code are available;
- Assess whether and how the CSP Cloud Services satisfy the security requirements as set out in the Code;
- Ensure the availability of any relevant elements of a:
  - Data retention policy;
  - Data breach management policy;
- Ensure that any of the personnel involved in the processing of the Customer's personal data (irrespective of their exact legal qualification) are bound by confidentiality agreements;
- Finalise the process by either:
  - Completing a self-assessment and providing a declaration of adherence (see Annex A) to a Competent Monitoring Body;
  - Undergoing a third-party certification and providing a declaration of adherence;
- Ensure that the outcome is appropriately reflected in the Code's public register;
- Ensure that the Cloud Service(s) (families) for which adherence has been declared are unambiguously identified as such.

ANNEX C

Controls Catalogue

- CONFIDENTIAL CONTENT: NOT PUBLICLY AVAILABLE -